

Par les gosses battus, par l'ivrogne qui rentre  
 Par l'âne qui reçoit des coups de pied au ventre  
 Et par l'humiliation de l'innocent châtié  
 Par la vierge vendue qu'on a déshabillée  
 Par le fils dont la mère a été insultée

Je vous salue, Marie<sup>1</sup>

*To Theres and Seraina*

## LEOPOLDT'S CONJECTURE FOR CM FIELDS

PREDA MIHĂILESCU

ABSTRACT. The conjecture of Leopoldt states that the  $p$ -adic regulator of a number field does not vanish. It was proved for the abelian case in 1967 by Brumer, using Baker theory. We prove this conjecture for CM number fields  $\mathbb{K}$ . The proof uses Iwasawa's methods – especially Takagi Theory – for deriving his skew symmetric pairing, together with Kummer- and Class Field Theory.

### CONTENTS

|  |    |
|--|----|
| 1. Introduction                              | 2  |
| 1.1. General notations                       | 3  |
| 1.2. Plan of the paper                       | 7  |
| 2. Radicals and Kummer theory                | 7  |
| 2.1. Growth of $\Lambda$ -modules            | 7  |
| 2.2. Radicals, projective limits and classes | 8  |
| 2.3. Classes as radicals and Kummer pairings | 8  |
| 2.4. Some important subfields of $\Omega_E$  | 11 |
| 3. Proof of Theorem 1                        | 12 |
| 3.1. A totally unramified $T$ -extension     | 13 |
| 3.2. The finiteness of $\mathbf{B}^+$        | 18 |
| 4. Appendix: Auxiliary results               | 21 |
| 4.1. Proof of Proposition 1                  | 21 |
| 4.2. Proof of Proposition 2                  | 25 |
| References                                   | 27 |

---

<sup>1</sup>Francis James: *Prière*. Music by Georges Brassens

*Date:* Version 1.0 January 23, 2013.

*Key words and phrases.* 11R23 Iwasawa Theory, 11R27 Units.

## 1. INTRODUCTION

Let  $\mathbb{K}/\mathbb{Q}$  be a finite galois CM extension with group  $\Delta$ . We denote as usual  $\mathbb{K}_\infty$  the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{K}$  and  $\mathbb{K}_n$  its intermediate fields,  $\Gamma = \text{Gal}(\mathbb{K}_\infty/\mathbb{K}) \cong \mathbb{Z}_p$  and  $\tau \in \Gamma$  a topological generator,  $T = \tau - 1$  and  $\Lambda = \mathbb{Z}_p[\Gamma] \cong \mathbb{Z}_p[[T]]$ . The  $p$ -parts of the ideal class groups of  $\mathbb{K}_n$  are  $A_n$  and  $A = \varprojlim_n A_n$ ; the groups  $A'_n, A'$  are defined like  $A_n, A$ , with respect to the ideal classes of the  $p$ -integers of  $\mathbb{K}_n$ . We let  $\mathbb{H}/\mathbb{K}_\infty$  be the maximal  $p$ -abelian unramified extension of  $\mathbb{K}_\infty$ : its Hilbert class field. Let  $\Omega_E = \cup_n \mathbb{K}_n[E(\mathbb{K}_n)^{1/p^{n+1}}]$ ,  $\Omega_{E'} = \cup_n \mathbb{K}_n[(E'(\mathbb{K}_n))^{1/p^{n+1}}]$ , with  $E(\mathbb{K}_n), E'(\mathbb{K}_n)$  the units, resp. the  $p$ -units of  $\mathbb{K}_n$ . We have proved in a separate paper [16] that the Iwasawa constant  $\mu$  vanishes for CM extensions, so we may assume that  $A$  has finite  $\mathbb{Z}_p$ -torsion. However the presence of infinite  $\mathbb{Z}_p$ -torsion can be easily dealt with in our context, so the methods may be generalized to extensions in which  $\mu = 0$  is not known, in particular for galois extensions which are not CM. We shall consider this in a separate paper, thus generalizing the results presented here by using some methods of representation theory which have been sketched in [15].

Dirichlet's unit theorem states that, up to torsion made up by the roots of unity  $W(\mathbb{K}) \subset \mathbb{K}^\times$ , the units  $E = \mathcal{O}(\mathbb{K})^\times$  are a free  $\mathbb{Z}$ -module of  $\mathbb{Z}$ -rank  $r_1 + r_2 - 1$ . As usual,  $r_1$  and  $r_2$  are the numbers of real, resp. pairs of complex conjugate embeddings  $\mathbb{K} \hookrightarrow \mathbb{C}$ . Let  $p$  be a rational prime. We consider the set  $P = \{\wp \subset \mathcal{O}(\mathbb{K}) : (p) \subset \wp\}$  of distinct prime ideals above  $p$  and let

$$\mathfrak{K}_p = \mathfrak{K}_p(\mathbb{K}) = \prod_{\wp \in P} \mathbb{K}_\wp = \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

be the product of all completions of  $\mathbb{K}$  at primes above  $p$ . Let  $\iota : \mathbb{K} \hookrightarrow \mathfrak{K}_p$  be the diagonal embedding. We write  $\iota_\wp(x)$  for the projection of  $\iota(x)$  in the completion at  $\wp \in P$ . If  $y \in \mathfrak{K}_p$ , then  $\iota_\wp(y)$  is simply the component of  $y$  in  $\mathbb{K}_\wp$ . If  $U \subset \mathfrak{K}_p^\times$  is the group of units, thus the product of local units at the same completions, then  $E$  embeds diagonally via  $\iota : E \hookrightarrow U$ . Furthermore one can use  $\iota$  for inducing a galois structure on  $\mathfrak{K}_p$  (see §2.1).

Let  $\overline{E} = \overline{\iota(E)} \subset U$  be the closure of  $\iota(E)$ ; this is a  $\mathbb{Z}_p$ -module with  $\mathbb{Z}_p\text{-rk}(\overline{E}) \leq \mathbb{Z}\text{-rk}(E) = r_1 + r_2 - 1$ . The difference

$$\mathcal{D}(\mathbb{K}) = (\mathbb{Z}\text{-rk}(E)) - (\mathbb{Z}_p\text{-rk}(\overline{E}))$$

is called the *Leopoldt defect*. The defect is positive if relations between the units arise in the local closure, which are not present in the global case. Equivalently, if the  $p$ -adic regulator of  $\mathbb{K}$  vanishes.

Leopoldt suggested in [13] that  $\mathcal{D}(\mathbb{K}) = 0$  for all number fields  $\mathbb{K}$ . This conjecture of Leopoldt was proved for abelian extensions by Brumer [5] in 1967, using a result of Ax [3] and a local version of Baker's linear forms in logarithms [4]. It is still open for arbitrary non abelian extensions. Since 1967 various attempts have been made for extending the results of [5] to non abelian extensions, using class field theory, Diophantine approximation

or both. The following very succinct list is intended to give an overview of various approaches rather than a extensive list of results on Leopoldt's conjecture. In [8], Greenberg notes for the first time a relation between the Leopoldt Conjecture and a special case of the Greenberg Conjecture: he shows that Leopoldt's Conjecture implies that  $A(T)$  (see §1.1. for the definitions) is finite for totally real fields, i.e. the Greenberg Conjecture holds for the  $T$  - part. Our central result, presented in Proposition 3 sharpens this observation to an equivalence: Leopoldt's conjecture holds for totally real fields iff  $\mathbf{B}$  is finite.

Emsalem, Kisilevsky and Wales [6] use group representations and Baker theory for proving the Conjecture for some small non abelian groups; this direction of research has been continued in some further papers by Emsalem or Emsalem and coauthors. Jaulent proves in [11] the Conjecture for some fields of small discriminants, using the *phantom* field  $\Phi$  which we shall define below. Currently the strongest result based on Diophantine approximation was achieved by Waldschmidt [20], who proved that if  $r$  is the  $\mathbb{Z}$  - rank of the units in the field  $\mathbb{K}$ , then the Leopoldt defect satisfies  $\mathcal{D}(\mathbb{K}) \leq r/2$ .

The connection of Leopoldt's conjecture to class field theory was already noted by Iwasawa in [9]. He shows that if  $\mathbb{K}_\infty$  is the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{K}$  and  $\Omega(\mathbb{K}) \supset \mathbb{K}_\infty$  is the maximal  $p$ -abelian  $p$ -ramified extension of  $\mathbb{K}$ , then  $\text{Gal}(\Omega(\mathbb{K})/\mathbb{K}) \sim \mathbb{Z}_p^n$ , where  $n = r_2 + 1 + \mathcal{D}(\mathbb{K})$ ; the proof of this fact is in any text book on cyclotomy and Iwasawa theory. For CM extensions  $\mathbb{K}$ , the conjecture herewith reduces to  $\Omega(\mathbb{K}^+) = \mathbb{K}_\infty^+ \cdot \mathbb{H}_1$ , where  $\mathbb{H}_1$  is the  $p$ -part of the Hilbert class field of  $\mathbb{K}^+$ . In this paper we shall use this equivalent statement and prove:

**Theorem 1.** *Let  $\mathbb{K}/\mathbb{Q}$  be a galois CM extension. Then the Leopoldt defect  $\mathcal{D}(\mathbb{K}) = 0$ .*

It is easy to show that if  $\mathbb{K}'/\mathbb{Q}$  is a field such that Leopoldt's Conjecture holds for some galois extension  $\mathbb{K}/\mathbb{Q}$  which contains  $\mathbb{K}'$ , then it holds for  $\mathbb{K}'$ . See for instance the final remark on p. 108 of Laurnt's paper [12]. We may thus concentrate on galois extensions of  $\mathbb{Q}$  and shall assume in the rest of this paper that  $\mathbb{K}/\mathbb{Q}$  is CM, galois and contains the  $p$ -th roots of unity. The Dirichlet number is  $r = r_2 - 1$  and  $\mathbb{Z}_p\text{-rk}(\overline{E}) = r_p = r - \mathcal{D}(\mathbb{K})$ . Furthermore, we assume that  $\mathbb{K}$  is such that all the primes above  $p$  are totally ramified in the  $\mathbb{Z}_p$  - cyclotomic extension  $\mathbb{K}_\infty/\mathbb{K}$  and the Leopoldt defect is constant for all intermediate fields of this extension. This can be achieved by choosing  $\mathbb{K}$  sufficiently large, according to [21], Lemma 13.30; although the field  $F$  is assumed in the respective section of Washington's book to be totally real, the proof of 13.30 does not depend on this assumption.

**1.1. General notations.** Let  $\mathbb{K}_\infty/\mathbb{K}$  be the cyclotomic  $\mathbb{Z}_p$  - extension of  $\mathbb{K}$  and  $\mathbb{K}_n$  the intermediate fields of level  $n$ . If  $\mathbb{B}_\infty$  is the cyclotomic  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$  and  $\mathbb{B}_n$  are its intermediate fields, then  $\mathbb{K}_n = \mathbb{K} \cdot \mathbb{B}_n$  and  $\mathbb{K}_\infty = \mathbb{B} \cdot \mathbb{K}$ . The ground field is  $\mathbb{K}$ , a complex galois extension with group

$\Delta = \text{Gal}(\mathbb{K}/\mathbb{Q})$ , which contains the  $p^k$ -th but not the  $p^{k+1}$ -th roots of unity. The constant  $k$  will be fixed in Definition 1 below, such that the  $\Lambda$ -modules related to  $\mathbb{K}$  have some useful additional properties. We write  $\mathbb{K} = \mathbb{K}_1 = \mathbb{K}_2 = \dots = \mathbb{K}_k$ . Note that our choice of  $k$  implies that  $\mathbb{B}_{k-1} \subset \mathbb{K}$  but  $\mathbb{B}_k \not\subset \mathbb{K}$ . As usual, we let  $\tau$  be a topological generator of  $\Gamma = \text{Gal}(\mathbb{K}_\infty/\mathbb{K})$  and  $T = \tau - 1$ ,  $\Lambda = \mathbb{Z}_p[[T]]$ . We assume that the Leopoldt defect  $\mathcal{D}(\mathbb{K}_n)$  is constant for all  $n \geq k$ . We let  $\zeta_{p^n} \in \mathbb{K}_n$  be a fixed, norm coherent sequence of  $p^n$ -th roots of unity. For some field  $K$  we write  $E(K), E'(K)$  for the units respectively the  $p$ -units of  $K$ , but we may also write  $E_n = E(\mathbb{K}_n)$ .

Moreover  $A(K), A'(K)$  are the  $p$ -parts of the ideal class groups of the integers and  $p$ -integers, and  $U(K)$  are the local 1-units, thus the integers of  $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$  which are congruent to one modulo uniformizers, in each completion. We let  $\overline{E}(K) = \cap_{N=1}^{\infty} E^{q-1} \cdot U(K)^{p^N} \subset U(K)$ , where  $q = \sharp U_{\wp}/\pi U_{\wp}$  is the degree of the residual field of any completion of  $\mathbb{K}$  at a prime above  $p$ . We write  $U'(K) = \{u \in U^+(K) : N_{K/\mathbb{Q}}(u) = 1\}$  for the norm-one units and  $W(K) = W(U(K))$  for the  $\mathbb{Z}_p$ -torsion of  $U(K)$ .

In particular, when  $K = \mathbb{K}_n$ , we define the limits  $E_\infty = \cup_n E(\mathbb{K}_n), U_\infty = \cup_n (U(\mathbb{K}_n))$ . Local class field theory shows that  $\text{Ker}(N : U_\infty \rightarrow U(\mathbb{K})) \subset \mathbb{Z}_p$ , since the kernel is invariant under the augmentation of  $\text{Gal}(\mathbb{K}_n/\mathbb{Q})$  for all  $n$ . Therefore,  $U'_\infty$  can also be defined as a projective limit under the norm maps. Since  $U(\mathbb{K}_n)$  is a pseudocyclic  $\mathbb{Z}_p[\text{Gal}(\mathbb{K}_n/\mathbb{Q})]$ -module at every finite level, it follows that  $U'_\infty$  is also a pseudocyclic  $\Lambda[\Delta]$ -module. The module  $W_\infty \cong \mathbb{Z}_p^s$ , where  $s$  is the number of primes above  $p$  in  $\mathbb{K}$ . The module  $U'(\mathbb{K}_n)$  is the smallest natural submodule in which the global units embed, in the sense that  $\mathbb{Z}_p\text{-rk}(U'(\mathbb{K}_n)) = \mathbb{Z}\text{-rk}(E(\mathbb{K}_n))$  and  $\overline{E}(\mathbb{K}_n) \hookrightarrow U'(\mathbb{K}_n)$ . The Leopoldt Conjecture will then show that the index of  $\overline{E}(\mathbb{K}_n)$  is finite and we already know that

$$\mathbb{Z}_p\text{-rk}(U'(\mathbb{K}_n)/U'(\mathbb{K})) = \mathbb{Z}_p\text{-rk}(\overline{E}(\mathbb{K}_n)/\overline{E}(\mathbb{K})),$$

since we assumed that the Leopoldt defect is stationary.

We assume that the primes above  $p$  are totally ramified in  $\mathbb{K}_\infty/\mathbb{K}$  and  $\wp \subset \mathbb{K}$  is one such prime. We let  $C = \Delta/D(\wp)$  be a set of coset representatives of the decomposition group of  $\wp$  in  $\Delta$  and  $\mathcal{P} = \{\nu\wp : \nu \in C\}$  the set of primes of  $\mathbb{K}$  above  $p$ . The completion of  $\mathbb{K}$  at  $\nu\wp$  is  $\mathbb{K}_{1,\nu\wp}$  and since  $\wp$  is totally ramified, it makes sense to write  $\mathbb{K}_{n,\wp}$  for the completion of  $\mathbb{K}_n$  at the unique ramified prime of  $\mathbb{K}_n$  above  $\wp$ . We let

$$\mathfrak{K}_n = \mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\nu \in C} \mathbb{K}_{n,\nu\wp},$$

a galois algebra in which  $\mathbb{K}_n$  is dense under the product topology; the projections to the completions at  $\nu\wp$  are denoted by  $\iota_{\nu\wp} : \mathfrak{K}_n \rightarrow \mathbb{K}_{n,\nu\wp}$ . There is an embedding  $\text{Gal}(\mathbb{K}_n/\mathbb{Q}) \hookrightarrow \text{Gal}(\mathfrak{K}_n/\mathbb{Q}_p)$ : indeed, if  $\mathbb{K}_n = \mathbb{Q}[\theta]$  as a simple algebraic extension and  $g(X)$  is the minimal polynomial of  $\theta$ , then  $\mathfrak{K}_n = \mathbb{Q}_p[X]/(g(X))$  as an algebra. For each  $\sigma \in \text{Gal}(\mathbb{K}_n/\mathbb{Q})$  there is a polynomial  $F_\sigma(X)$  with  $\sigma(\theta) = F_\sigma(\theta)$ . If  $\Theta = X + (g(X)) \in \mathfrak{K}_n$ , then

the map  $\iota(\sigma) : h(\Theta) \mapsto h(F_\sigma(\Theta))$  is an automorphism of  $\mathfrak{K}_n$  which restricts to  $\sigma$ . If  $\pi \in \mathbb{K}_n$  maps to a uniformizer in all completions, then  $U(\mathbb{K}_n) = \{x \in \mathcal{O}(\mathfrak{K}) : \iota_{\nu\varphi}(u) \equiv 1 \pmod{\nu\pi}\}$  and  $\overline{E}_n \subset U(\mathbb{K}_n)$  is the  $p$ -adic completion of the intersection of the diagonal embedding  $E_n \hookrightarrow \mathfrak{K}_n$  with  $U(\mathbb{K}_n)$ .

For all  $n \geq 1$  we let  $A_n$  be the  $p$ -Sylow subgroups of the class group  $\mathcal{C}(\mathbb{K}_n)$  and  $A$  the projective limit, a  $\Lambda$ -module. The groups  $A'_n, A'$  are defined like  $A_n, A$ , with respect to the class groups of the  $p$ -integers: see also [9], §4.3; the numeration respects the same rule as for the intermediate fields. The groups  $\mathbf{B}_n \subset A_n, \mathbf{B} \subset A[T]$  are those generated by classes of ideals containing ramified primes above  $p$ , resp. the projective limit of these groups. The norms  $N_{m,n} = \mathbf{N}_{\mathbb{K}_m/\mathbb{K}_n}$  for  $m > n \geq k$  are supposed to be surjective as maps  $A_m \rightarrow A_n$  and  $A'_m \rightarrow A'_n$ .

Let  $f(T) \in \mathbb{Z}_p[T]$  and  $M$  be some  $\Lambda$ -torsion module, written additively. We define

$$(1) M(f) = \{x \in M : \exists n \geq 0, f^n x = 0\}, \quad M[f] = \{x \in M : fx = 0\}.$$

If there is an  $m \geq 0$  such that  $f^m M = 0$ , then the order  $\text{ord}_f(M)$  is the least such integer. Otherwise  $\text{ord}_f(M) = \infty$ . Let  $R_f(M) = M(f)/(fM(f))$  and  $S_f(M) = M[f]$ . Assuming that these modules are finitely generated, we note that the exact sequence

$$0 \rightarrow S_f(M) \rightarrow M(f) \rightarrow M(f) \rightarrow R_f(M) \rightarrow 0,$$

in which the central arrow is induced by the map  $x \mapsto fx$  induces a pseudoisomorphism  $S_f(M) \sim R_f(M)$ . We let  $f - \text{rk}(M)$  be the common number of generators in a minimal system of generators of either  $R_f(M)$  or  $S_f(M)$ , as a  $\Lambda$ -module.

We let further  $\mathbb{H}, \Omega$  be the maximal  $p$ -abelian extensions of  $\mathbb{K}_\infty$ , which are unramified, respectively  $p$ -ramified. Note that we do not use the index  $\infty$  for  $\mathbb{H}$  and will write instead  $\mathbb{H}(\mathbb{K}) = \mathbb{H}_1$  for the Hilbert class field of  $\mathbb{K}$ . Complex conjugation acts by conjugation on the galois groups  $\text{Gal}(\mathbb{H}/\mathbb{K}_\infty), \text{Gal}(\Omega/\mathbb{K}_\infty)$ , inducing a splitting in disjoint extensions  $\mathbb{H} = \mathbb{H}^+ \cap \mathbb{H}^-, \Omega = \Omega^+ \cdot \Omega^-$  and  $\mathbb{H}^+ \cap \mathbb{H}^- = \Omega^+ \cap \Omega^- = \mathbb{K}_\infty$ . The maximal  $p$ -abelian unramified extension of  $\mathbb{K}_\infty$  which splits all the primes above  $p$  is  $\mathbb{H}' \subset \mathbb{H}$ . We have

$$\text{Gal}(\mathbb{H}/\mathbb{H}') \cong \mathbf{B} \quad \text{and} \quad \text{Gal}(\mathbb{H}'/\mathbb{K}_\infty) \cong A'.$$

We shall consider the following additional subfields of  $\Omega$ :

$$\Omega_E = \bigcup_{n \geq 0} \mathbb{K}_n \left[ E(\mathbb{K}_n)^{1/p^{n+1}} \right], \quad \Omega_{E'} = \bigcup_{n \geq 0} \mathbb{K}_n \left[ E'(\mathbb{K}_n)^{1/p^{n+1}} \right],$$

so  $\mathbb{K}_\infty \subset \Omega_E \subset \Omega_{E'} \subset \Omega$ . Moreover,  $\Omega_n \subset \Omega$  is the maximal  $p$ -abelian  $p$ -ramified extension of  $\mathbb{K}_n$ . Complex conjugation acts on  $\text{Gal}(\Omega_n/\mathbb{K}_n)$  inducing a splitting in the linear disjoint extensions  $\Omega_n^- \cdot \Omega_n^+ = \Omega_n$ . Then we

have by class field theory (e.g. [19], p. 144, Theorem 5.1)

$$(2) \quad \text{Gal}(\Omega_n/\mathbb{H}_n) \cong U(\mathbb{K}_n)/\overline{E}_n.$$

The isomorphism is given by the global Artin symbol  $\varphi : U(\mathbb{K}_n) \rightarrow \text{Gal}(\Omega_n/\mathbb{H}_n)$ . The Artin symbol is also well defined as a map  $\varphi : A_n \rightarrow \text{Gal}(\mathbb{H}_n/\mathbb{K}_n)$  via  $\varphi(a) = \left( \frac{\mathbb{H}_n/\mathbb{K}_n}{\Omega} \right), \Omega \in a$ . We shall use the same notation for the two Artin maps.

If  $X$  is a finite  $p$ -group, the exponent of  $X$  is the smallest power of  $p$  that annihilates  $X$ ; the *subexponent* is

$$\text{sexp}(X_p) = \min\{ \text{ord}(x) : x \in X \setminus X^p \}.$$

The general notations from Iwasawa theory which we use here are:

|                                   |   |
|-----------------------------------|---|
| $p$                               | A rational prime,   |
| $X^\circ$                         | The $\mathbb{Z}_p$ - torsion of the abelian group $X$ ,   |
| $\zeta_{p^n}$                     | Norm coherent sequence of primitive $p^n$ -th roots of unity,   |
| $\mu_{p^n}$                       | $\{\zeta_{p^n}^k, k \in \mathbb{N}\}$ ,   |
| $\mathbb{K}$                      | A CM galois extension of $\mathbb{Q}$ containing the $p$ -th roots of unity   |
| $\mathbb{K}_\infty, \mathbb{K}_n$ | The cyclotomic $\mathbb{Z}_p$ - extension of $\mathbb{K}$ , resp. its $n$ -th intermediate field,                               |
| $\Delta$                          | $\text{Gal}(\mathbb{K}/\mathbb{Q})$ ,   |
| $s$                               | The number of primes above $p$ in $\mathbb{K}$ ,  |
| $\Gamma$                          | $\text{Gal}(\mathbb{K}_\infty/\mathbb{K}) = \mathbb{Z}_p\tau$ , $\tau$ a topological generator of $\Gamma$                      |
| $T$                               | $\tau - 1$ ,  |
| $*$                               | Iwasawa's involution on $\Lambda$ induced by $T^* = (p^{k+1} - T)/(T + 1)$ ,  |
| $\Lambda$                         | $\mathbb{Z}_p[[T]]$ , $\Lambda_n = \Lambda/(\omega_n \Lambda)$ ,  |
| $\omega_n$                        | $(T + 1)^{p^{n-(k+1)}} - 1$ , $(\mathbb{K}_n^\times)^{\omega_n} = \{1\}$ ,  |
| $N_{m,n}$                         | $\mathbf{N}_{\mathbb{K}_m/\mathbb{K}_n} = \mathbf{N}_{\mathfrak{K}_m/\mathfrak{K}_n}$ ; $N_n = N_{\mathbb{K}_n/\mathbb{K}}$ ,   |
| $M(f)$                            | = The $f$ -part of the $\Lambda$ -module $M$ , with $f \in \mathbb{Z}_p[T]$ ,   |
| $M[f]$                            | = The $f$ -torsion of the $\Lambda$ -module $M$ , with $f \in \mathbb{Z}_p[T]$ ,  |
| $A_n = A(\mathbb{K}_n)$           | The $p$ - part of the ideal class group of $\mathbb{K}_n$ ,   |
| $A$                               | $\varprojlim A_n$ ,   |
| $A'_n = A'(\mathbb{K}_n)$         | The $p$ - part of the ideal class group of the $p$ - integers of $\mathbb{K}_n$ ,   |
| $A'$                              | $\varprojlim A'_n$ ,  |
| $\mathcal{D}(\mathbb{K})$         | The Leopoldt defect of the field $\mathbb{K}$ ,   |
| $\mathbf{B}$                      | $\{b = (b_n)_{n \in \mathbb{N}} \in A : \text{The classes } b_n \text{ contain products of ramified primes}\}_{\mathbb{Z}_p}$ , |
| $\Omega$                          | The maximal $p$ - abelian $p$ - ramified extension of $\mathbb{K}_\infty$ ,   |
| $\Omega(\mathbb{K}_n)$            | The maximal $p$ - abelian $p$ - ramified extension of $\mathbb{K}_n$ ,  |
| $\Omega_E$                        | $\cup_{n=0}^\infty \mathbb{K}_n[E(\mathbb{K}_n)^{1/p^{n+1}}] = \mathbb{K}_\infty[E^{1/p^\infty}]$ ,                             |
| $\Omega_{E'}$                     | $\cup_{n=0}^\infty \mathbb{K}_n[E'(\mathbb{K}_n)^{1/p^{n+1}}] = \mathbb{K}_\infty[E'^{1/p^\infty}]$ ,                           |
| $\mathbb{H}$                      | The maximal $p$ - abelian unramified extension of $\mathbb{K}_\infty$ ,   |
| $\mathbb{H}' \subset \mathbb{H}$  | The maximal subextension of $\mathbb{H}$ which splits all the primes above $p$ .  |

**1.2. Plan of the paper.** Our approach can be sketched as follows: assuming that  $\mathcal{D}(\mathbb{K}) \neq 0$ ,

- A. We show in chapter 2 that the  $T^*$ -part of  $A^-$  is non trivial and  $\Omega^-(\mathbb{K}_n) \subset \Omega_E \cdot \mathbb{H}^-$  for all  $n > 0$ . The second result implies that  $(A')^+[T]$  is finite, via a Lemma of Iwasawa, which we shall prove also separately in Chapter 3. We also investigate radicals of Kummer extensions in projective limits, giving appropriate definitions and properties of extensions  $\mathbb{K}_\infty \subset \mathbb{L} \subset \mathbb{K}_\infty[(A^-)^{1/p^\infty}]$  and  $\Omega_{E'} \subset \mathbb{L} \subset \Omega_{E'}[(A^+)^{1/p^\infty}]$ .
- B. The main result of Chapter 3 is Proposition 3 in which we show that  $\mathbb{K}_\infty[(A^-(T^*))^{1/p^\infty}] \subset \mathbb{H}^+$ , thus proving the equivalence of Leopoldt's conjecture to the finiteness of  $\mathbf{B}^+$ .
- C. Finally we prove that  $\mathbf{B}^+$  is finite by some arguments of galois and class field theory.

## 2. RADICALS AND KUMMER THEORY

In this chapter we shall derive some useful facts about the growth of cyclic,  $\mathbb{Z}_p$ -free  $\Lambda$ -modules  $\Lambda a$ , which allow a canonical definition of extensions like  $\mathbb{K}_\infty[(\Lambda a)^{1/p^\infty}]$  for  $a \in A^-$  and  $\Omega_E[(\Lambda a)^{1/p^\infty}]$  for  $a \in A^+$ , together with the finite level Kummer extensions contained in these fields. Some of the results in this chapter have been exposed in a previous paper [17]; they will be reviewed here, the proofs being provided in the Appendix.

**2.1. Growth of  $\Lambda$ -modules.** The following proposition describes the growth of the order of elements  $a_n \in A_n$ , within given norm coherent sequences.

**Proposition 1.** *Let  $\mathbb{K}$  be a galois CM extension containing the  $p$ -th roots of unity and  $A_n, A$  be defined like above and let  $q = p^M$  annihilate the  $\mathbb{Z}_p$ -torsion of  $A_n$ . There is an  $n_0 > 0$  such that*

$$p\text{-rk}(A_n^q) = p\text{-rk}(A_{n_0}^q) = \lambda(A).$$

*Moreover, if  $a = (a_n)_{n \in \mathbb{N}} \in A$  has infinite order and  $\Lambda a$  is a free  $\mathbb{Z}_p$ -module of finite rank, then the ideal lift map  $\iota_{n,n+1} : \Lambda a_n \rightarrow \Lambda a_{n+1}$  is injective for all  $n \geq n_0$  and*

$$(3) \quad a_{n+1}^p = \iota_{n,n+1}(a_n), \quad a_{n+1}^{\omega_n} \in \iota_{n,n+1}(A_n^-[p]).$$

*In particular, there is a smallest integer  $z \geq 0$  such that for all  $n > n_0$ ,  $\text{ord}(a_n) \leq p^{n+z}$  and*

$$(4) \quad \nu_{n+1,n}(a_{n+1}) = a_{n+1}^p = \iota_{n,n+1}(a_n).$$

We shall write  $n' = n + z$  for  $n > n_0$ . The proposition implies in particular that for  $n > n_0$ , the extensions  $\mathbb{H}_n \cdot \mathbb{K}_{n'}$  are Kummer over  $\mathbb{K}_{n'}$ . With this we define the value  $k$ :



**Definition 1.** We let  $\mathbb{K}$  be such that  $n_0 = 1$  and the Leopoldt defect is stable for all  $n > 1$ . Moreover, we assume that for  $a = (a_n)_{n \in \mathbb{N}} \in A$  with  $\Omega_E[a^{1/p^\infty}]$  not totally unramified, we have

$$\left[ \Omega_E[a^{1/p^\infty}] \cap (\Omega_E \cdot \mathbb{H}) : \Omega_E \right] = \left[ \Omega_E[a_1^{1/\text{ord}(a_1)}] \cap (\Omega_E \cdot \mathbb{H}) : \Omega_E \right];$$

the precise definition of these extensions will be given in the section below. The base field  $\mathbb{K}$  will be chosen such that the Leopoldt defect is constant above  $\mathbb{K}$  and all the above condition hold. Then  $k > 0$  is the largest integer such that  $\zeta_{p^k} \in \mathbb{K}$ .

**2.2. Radicals, projective limits and classes.** Let  $\mathbb{L}/\mathbb{K}_n$  be a finite Kummer extension of exponent  $q = p^m, m \leq n$ . Its classical Kummer radical  $\text{rad}(\mathbb{L}/\mathbb{K}_n) \subset \mathbb{K}_n^\times$  is a multiplicative group containing  $(\mathbb{K}_n^\times)^q$  such that  $\mathbb{L} = \mathbb{K}_n[\text{rad}(\mathbb{L}/\mathbb{K}_n)^{1/q}]$  (e.g. [18], Chapter VIII, §8). Following Albu [1], we define the *cogalois* radical

$$(5) \quad \text{Rad}(\mathbb{L}/\mathbb{K}_n) = \left( [\text{rad}(\mathbb{L}/\mathbb{K}_n)^{1/q}]_{\mathbb{K}_n^\times} \right) / \mathbb{K}_n^\times,$$

where  $[\text{rad}(\mathbb{L}/\mathbb{K}_n)^{1/q}]_{\mathbb{K}_n^\times}$  is the multiplicative  $\mathbb{K}_n^\times$ -module spanned by the roots in  $\text{rad}(\mathbb{L}/\mathbb{K}_n)^{1/q}$  and the quotient is one of multiplicative groups. Then  $\text{Rad}(\mathbb{L}/\mathbb{K}_n)$  has the useful property of being a finite multiplicative group isomorphic to  $\text{Gal}(\mathbb{L}/\mathbb{K}_n)$ . For  $\rho \in \text{Rad}(\mathbb{L}/\mathbb{K}_n)$  we have  $\rho^q \subset \text{rad}(\mathbb{L}/\mathbb{K}_n)$ ; therefore, the Kummer pairing is naturally defined on  $\text{Gal}(\mathbb{L}/\mathbb{K}_n) \times \text{Rad}(\mathbb{L}/\mathbb{K}_n)$  by

$$\langle \sigma, \rho \rangle_{\text{Rad}(\mathbb{L}/\mathbb{K}_n)} = \langle \sigma, \rho^p \rangle_{\text{rad}(\mathbb{L}/\mathbb{K}_n)}.$$

Kummer duality induces a twisted isomorphism of  $\text{Gal}(\mathbb{K}_n/\mathbb{Q})$  - modules  $\text{Rad}(\mathbb{L}/\mathbb{K}_n)^\bullet \cong \text{Gal}(\mathbb{L}/\mathbb{K}_n)$ . Here  $g \in \text{Gal}(\mathbb{K}_n/\mathbb{Q})$  acts via conjugation on  $\text{Gal}(\mathbb{L}/\mathbb{K}_n)$  and via  $g^* := \chi(g)g^{-1}$  on the twisted module  $\text{Rad}(\mathbb{L}/\mathbb{K}_n)^\bullet$ ; we denote this twist the *Leopoldt involution*. It reduces on  $\text{Gal}(\mathbb{K}_n/\mathbb{K})$  to the classical Iwasawa involution (e.g. [19], p. 150).

Suppose now that  $\mathbb{L} \subset \Omega$  is an infinite extension of  $\mathbb{K}_\infty$  which is galois over  $\mathbb{K}$  and let  $L = \text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ , which is a  $\Lambda$ -module. Let  $\mathbb{L}_n = \mathbb{L} \cap \underline{\Omega}_n$ , where  $\underline{\Omega}_n \subset \mathbb{K}_{n'} \cdot \Omega_n$  is the maximal Kummer extension of  $\mathbb{K}_{n'}$  contained in  $\mathbb{K}_{n'} \cdot \Omega_n$  and galois over  $\mathbb{K}$ . Then  $\mathbb{L} = \cup_n \mathbb{L}_n$  and  $L = \varprojlim_n \text{Gal}(\mathbb{L}_n/\mathbb{K}_n)$ . The radicals  $R_n = \text{Rad}(\mathbb{L}_n/\mathbb{K}_{n'})$  form a projective system with respect to the twisted norms  $N_{m,n}^*$ , by Kummer duality. We let  $R = \varprojlim_n (R_n)$  and define  $\mathbb{K}_\infty[R] = \cup_n \mathbb{K}_\infty[R_n] = \cup_n \mathbb{L}_n = \mathbb{L}$ . In the case when  $\mathbb{L} \subset \mathbb{H}$  we know from Proposition 1 and the choice of  $\mathbb{K}$  that  $L_{n+1}^p = \iota_{n,n+1}(L_n)$  and thus  $R_n$  form a projective system with respect to the  $p$ -map too.

**2.3. Classes as radicals and Kummer pairings.** We now apply the definition of cogalois radicals in the setting of Hilbert class fields. We let  $a = (a_n)_{n \in \mathbb{N}} \in A$  be such that  $\Lambda a$  is an infinite module of finite  $\mathbb{Z}_p$ -rank. The purpose of this section is to investigate the extensions  $\Omega_{E'}[(\Lambda a)^{1/p^\infty}]$  for  $a \in A$  and, in the case when  $a \in A^-$ , also the natural extensions  $\mathbb{K}_\infty[(\Lambda a)^{1/p^\infty}]$ .



We show in particular that these notations are well defined. Let  $z \geq 0$  be the smallest integer such that  $\text{ord}(a_n) \leq p^{n+z}$  for all  $a = (a_n)_{n \in \mathbb{N}} \in A$  and all  $n \geq 0$ , and there is at least one sequence for which equality holds.

For  $a = (a_n)_{n \in \mathbb{N}}$ , we define a map  $\beta : a_n \rightarrow \mathbb{K}_n^\times / (E_n \cdot (\mathbb{K}_n^\times)^{p^{n+z}})$ , called the *instantiation map*, as follows: let  $\mathfrak{A} \in a_n$  and  $\alpha_n = \alpha(a_n, \mathfrak{A}) \in \mathbb{K}_n^\times$  with  $(\alpha_n) = \mathfrak{Q}^{p^{n+z}}$ . Then  $\alpha(a_n, \mathfrak{Q})$  is an *explicit instantiation* of the class  $a_n$  at the ideal  $\mathfrak{A}$  and  $\beta(a_n)$  is the image of  $\alpha_n$  in  $\mathbb{K}_n^\times / (E_n \cdot (\mathbb{K}_n^\times)^{p^{n+z}})$ . One verifies that  $\alpha_n$  is well defined modulo  $E_n \cdot (\mathbb{K}_n^\times)^{p^{n+z}}$ , hence  $\beta(a_n) = \alpha_n \bmod E_n \cdot (\mathbb{K}_n^\times)^{p^{n+z}}$  is well defined too. With this, for all integers  $m \leq n+z$ , we let

$$(6) \quad \Omega_{E'}[a_n^{1/p^m}] = \Omega_{E'}[\alpha_n^{1/p^m}],$$

which is an extension unramified outside  $p$  and which only depends on  $a_n$  but not on the choice of  $\alpha_n$ . We define in the same way  $\Omega_{E'}[(\Lambda a_n)^{1/p^m}] = \Omega_{E'}[\alpha_n^{\Lambda/p^m}]$ . If  $\Lambda a$  is infinite of finite  $p$ -rank, we have by (3) that

$$\Omega_{E'}[(\Lambda a_n)^{1/\text{ord}(a_n)}] = \Omega_{E'}[(\Lambda a_{n+1})^{p/\text{ord}(a_{n+1})}] \subset \Omega_{E'}[(\Lambda a_{n+1})^{1/\text{ord}(a_{n+1})}].$$

Letting  $\mathbb{L}'_{n,a} = \Omega_{E'}[(\Lambda a_n)^{1/\text{ord}(a_n)}]$ , we see that the sequence  $\mathbb{L}'_{n,a}$  is injective and define

$$\mathbb{L}'_a = \cup_n \mathbb{L}'_{n,a} = \Omega_{E'}[(\Lambda a)^{1/p^\infty}].$$

We note that the extensions above only depend on the module  $\Lambda a$  but not on particular generators thereof; the same holds at finite levels.

We also have  $\Omega = \Omega_{E'}[A^{1/p^\infty}]$ , so for  $\Omega_{E'} \subset \mathbb{L} \subset \Omega$  there is some subgroup  $B \subset A$  with  $\mathbb{L} = \Omega_{E'}[B^{1/p^\infty}]$ ; if  $\mathbb{L}/\mathbb{K}$  is galois, then  $B$  is a  $\Lambda$ -module. We call the module  $B$  the *class - radical* of  $\mathbb{L}$  and write

$$(7) \quad \text{C-Rad}(\mathbb{L}/\Omega_{E'}) = B \subset A \quad \Leftrightarrow \quad \mathbb{L} = \Omega_{E'}[B^{1/p^\infty}].$$

We let  $\overline{\mathbb{H}} = \Omega_{E'} \cdot \mathbb{H} \subset \Omega$  and  $\overline{\mathbb{H}}' = \Omega_{E'} \cdot \mathbb{H}' \subset \Omega$ . If  $\overline{X} = \text{Gal}(\Omega/\mathbb{H})$  and  $\mathbb{H}_E = \mathbb{H} \cap \Omega_{E'}$ , then  $\overline{X}$  acts by restriction on fields  $\Omega_{E'} \subset \mathbb{L}' \subset \Omega$ , and letting  $\mathbb{L} = (\mathbb{L}')^{\overline{X}}$  be the fixed fields of these restrictions, we have  $\mathbb{H}_E = \Omega_{E'}^{\overline{X}} \subset \mathbb{L} \subset \mathbb{H} \subset \Psi := \Omega^{\overline{X}}$  and  $\text{Gal}(\mathbb{L}/\mathbb{H}_E) = \text{Gal}(\mathbb{L}'/\Omega_{E'})$ . In this way we obtain a canonical definition of

$$(8) \quad \mathbb{H}_E[(\Lambda a)^{1/p^\infty}] = \left( \Omega_{E'}[(\Lambda a)^{1/p^\infty}] \right)^{\overline{X}}, \quad \text{with} \\ \text{Gal}(\mathbb{H}_E[(\Lambda a)^{1/p^\infty}]/\mathbb{H}_E) \cong \text{Gal}(\Omega_{E'}[(\Lambda a)^{1/p^\infty}]/\Omega_{E'}).$$

The subextensions  $\mathbb{H}_E[a^{1/p^\infty}]$  are also defined accordingly, as fixed fields of the restriction of  $\overline{X}$ .

We define maps  $\ell : A \rightarrow \mathbb{N}$  and  $\ell : A_n \rightarrow \mathbb{N}$  as follows: for  $a = (a_n)_{n \in \mathbb{N}} \in A$ , let

$$(9) \quad \ell(a_n) = v_p \left( \left[ \Omega_{E'}[a_n^{1/p^{n+z}}] \cap \overline{\mathbb{H}} : \Omega_{E'} \right] \right) \leq v_p(\text{ord}(a_n)).$$

The map  $\ell(a_n)$  is an increasing function on  $n$  and we let at infinity,

$$\ell(a) = \begin{cases} \infty & \text{if } \Omega_E[a^{1/p^\infty}] \subset \Omega_E \cdot \mathbb{H} \\ v_p([\Omega_E[a^{1/p^\infty}] \cap (\Omega_E \cdot \mathbb{H}) : \Omega_E]) & \text{otherwise.} \end{cases}$$

For  $a_n, b_n \in A_n$  with  $\ell(a_n) \neq \ell(b_n)$  we have

$$\ell(a_n \cdot b_n) = \min(\ell(a_n), \ell(b_n));$$

in particular  $\ell(ab) = \infty$  iff  $\ell(a) = \ell(b) = \infty$ . The space

$$(10) \quad \mathcal{L}(A') = \{a \in A' : \ell(a) = \infty\} \subset A'$$

is a  $\Lambda$ -submodule, due to the previous multiplicative relation. It is an important module, which was first investigated by Iwasawa in the context of the definition of his *skew symmetric pairing*. There is one additional condition in Iwasawa's definition of his linear space, namely

$$\mathcal{L}_I(A') = \{a \in \mathcal{L}(A') : \Omega_{E'}[a^{1/p^\infty}] \subset \overline{\mathbb{H}}'\}.$$

We shall see briefly, that another equivalent formulation of Leopoldt's conjecture states that  $\mathcal{L}(A') = \mathcal{L}_I(A')$ , or  $\mathbf{B}^+$  is finite.

In Lemma 14 of [9] Iwasawa shows that  $\mathcal{L}_I(A')[T] = \{1\}$ . Combined with our Theorem 2 below, which states that  $\Omega^- \subset \mathbb{H}^- \cdot \Omega_{E'}$  this implies plainly that  $(A')^+(T)$  is finite. Indeed, this theorem implies that if  $a \in (A')^+[T]$ , then  $\Omega_{E'}[a^{1/p^\infty}] \subset \Omega_{E'} \cdot \mathbb{H}$  is either a trivial extension, or it is totally unramified; the second contradicts Lemma 14, and therefore  $\Omega_{E'}[a^{1/p^\infty}] = \Omega_{E'}$ , so  $a$  must have finite order. We note this fact for future reference and will give in Chapter 3 below an independent proof of:

**Lemma 1.**

$$|(A')^+(T)| < \infty.$$

It turns out from Iwasawa's results that  $\mathcal{L}(A')$  is a self-dual space, and it is the obstruction space to Greenberg's conjecture. From reflection, one can readily see that Greenberg's conjecture holds iff  $(\mathcal{L}(A'))^- = \{1\}$ : indeed, the radical of  $\text{Rad}(\mathbb{H}^+/\mathbb{K}_\infty)$  can only be built from classes in  $A^-$ , and this radical is finite iff  $(\mathcal{L}(A'))^- = \{1\}$ . We shall investigate the relation between  $\mathcal{L}(A')$  and Greenberg's conjecture in a separate, subsequent paper, following the sketch given in [14].

If  $a \in A^-$ , then  $\alpha_n/\overline{\alpha_n}$  is well defined modulo  $\mu_{\text{ord}(a_n)} \cdot (\mathbb{K}^\times)^{\text{ord}(a_n)}$ . Since  $p \neq 2$  and  $a_n/\overline{a_n} = a_n^2$ , in this case the extensions  $\mathbb{K}_\infty[a_n^{1/p^n}]$  and  $\mathbb{K}_\infty[a^{1/p^\infty}]$  are also well defined. We have

$$(11) \quad \Omega^+ = \mathbb{K}_\infty[(A^-)^{1/p^\infty}],$$

and the class radicals  $\text{C-Rad}(\mathbb{L}/\mathbb{K}_\infty)$  are defined for  $\mathbb{K}_\infty \subset \mathbb{L} \subset \Omega^+$  like in the general case 7.

We shall like to consider  $\mathbb{K}_{n'}[a_n^{1/p^{n+z}}]$ , for  $n'(n) = n + z$ . In this case there is some ambiguity in the choice of  $\alpha_n/\overline{\alpha_n}$  and we choose the implicit roots

of unity such that the degree  $[\mathbb{K}_{n'}[a_n^{1/p^{n+z}}] \cap \mathbb{H}_{n'} : \mathbb{K}_{n'}]$  is maximal. One verifies that this makes the extension unique.

Finally, we consider projective-projective Kummer pairings. Let  $\Omega_{E'} \subset \mathbb{L} \subset \Omega$  be a galois extension of  $\mathbb{K}$  and let  $B = \text{C-Rad}(\mathbb{L}/\Omega_{E'})$ ,  $X = \text{Gal}(\mathbb{L}/\Omega_{E'})$ , so  $B, X$  are dual, finitely generated  $\Lambda$ -torsion modules. For every finite level, we have a Kummer pairing  $\langle \cdot, \cdot \rangle_n : X_n \times B_n \rightarrow \mu_{p^{n+z}}$  defined for  $x = (x_n)_{n \in \mathbb{N}} \in X$  and  $b = (b_n)_{n \in \mathbb{N}} \in B$  as follows:

$$\langle x_n, b_n \rangle_n = \langle x_n, \beta(b_n) \rangle \in \mu_{p^{n+z}}.$$

Recall that  $B_n \subset (\mathbb{K}_{n+z}^\times)^{1/p^{n+z}}$  with  $\Omega_{E'}[B_n] = \mathbb{L}_n$ . By Proposition 3, the maps  $\nu_{n+1,n}$  are equal to  $p$ -maps for sufficiently large  $n$ , so the norms are compatible, by restriction. If  $W = T(\mu_{p^{n+z}})$  is the Tate module for the roots of unity, and  $\psi : W \rightarrow \mathbb{Z}_p$  be the natural projection. We obtain in the limit an additive projective-projective pairing

$$(12) [\cdot, \cdot] : X \times B \rightarrow \mathbb{Z}_p : (x, b) \mapsto \langle x, b \rangle = \psi \left( \varprojlim_n \langle x_n, b_n \rangle_n \right).$$

The pairing is by definition bilinear, non-degenerate and galois equivariant. If  $Y = \text{Gal}(\overline{\mathbb{H}}/\Omega_{E'})$ , then Iwasawa defines a projective-projective pairing only on  $Y \times Y$  by considering for  $y = (y_n)_{n \in \mathbb{N}}$  in the second component of the pairing first the preimages  $b_n = \varphi^{-1}(y_n) \in A'_n$ , passing to the *injective limit*  $\underline{A}' = \varprojlim_n A'_n$ , and then taking the Tate tower  $T(\underline{A}'[p^n])$ . Our construction is both more direct and more general, since it does not restrict to unramified extensions. In fact the construction holds for subfields of  $\mathbb{K}_\infty^{pab}$ , the maximal  $p$ -abelian extension of  $\mathbb{K}_\infty$ , but for our present purposes the above definition is sufficient.

**2.4. Some important subfields of  $\Omega_E$ .** We shall take here an approach to Leopoldt's conjecture, that uses class field and Iwasawa theory. As Iwasawa noted in [9],  $\mathbb{K}^+$  has  $\mathcal{D}(\mathbb{K}) + 1$  independent  $\mathbb{Z}_p$ -extensions, one of which is the cyclotomic one. The Leopoldt conjecture is thus equivalent to the fact that  $\mathbb{K}^+$  has no other  $\mathbb{Z}_p$ -extension except the cyclotomic, while  $\Omega(\mathbb{K}) = \Omega^-(\mathbb{K})$ . We have in general

**Proposition 2.**

$$\Omega_n^- \subset \Omega_{E'} \cdot \mathbb{H}_n.$$

*In particular, in the injective limit we have*

$$(13) \quad \Omega^- \subset \overline{\mathbb{H}}^- = \Omega_{E'} \cdot \mathbb{H}^-.$$

The relation (13) implies that

$$(14) \quad \Omega_{E'}[(A^+)^{1/p^\infty}] \subset \overline{\mathbb{H}},$$

thus the extensions with radicals in the real classes are unramified over  $\Omega_{E'}$ ; indeed,

$$\Omega_{E'}[(A^+)^{1/p^\infty}] = \Omega_{E'} \cdot \Omega^- \subset \Omega_{E'} \cdot \mathbb{H}^- \subset \Omega_{E'} \cdot \mathbb{H} = \overline{\mathbb{H}},$$

a fact which we shall use below for proving the Lemma 1.

We give an elementary, constructive proof of this proposition in the Appendix. Assuming that Leopoldt's Conjecture is false for  $\mathbb{K}$ , we have the following important consequence:

**Lemma 2.** *Let  $\mathbb{K}$  be like above and suppose that the Leopoldt defect  $\mathcal{D}(\mathbb{K}) > 0$ . Then*

$$\mathbb{Z}_p\text{-rk}(A^-[T^*]) = \mathcal{D}(\mathbb{K}).$$

*Proof.* If Leopoldt's conjecture fails, then  $\Omega^+(\mathbb{K})/\mathbb{K}_\infty$  is a product of  $\mathcal{D}(\mathbb{K})$  independent  $\mathbb{Z}_p$ -extensions. By reflection, their radicals stem from  $(\mathbb{K}_\infty^\times)^{1-j}$  and since this group contains no other units except for the roots of unity  $\mu_{p^\infty} \subset \mathbb{K}_\infty$ , it follows that the radical is built by classes. Since  $\text{C-Rad}(\Omega^+/\mathbb{K}_\infty) \cong \text{Gal}(\Omega^+/\mathbb{K}_\infty)^\bullet$  and the latter group is annihilated by  $T$ , it follows by reflection that  $\text{C-Rad}(\Omega^+/\mathbb{K}_\infty) \subset A^-[T^*]$ , in the sense of the definition of classes as radicals, given in the previous section. Conversely, we have seen that  $\mathbb{K}_\infty[(A^-[T^*])^{1/p^\infty}]$  is a well defined extension and it is abelian over  $\mathbb{K}$ , so the ranks

$$\mathbb{Z}_p\text{-rk}(A^-[T^*]) = \mathbb{Z}_p\text{-rk}(\text{Gal}(\Omega(\mathbb{K}^+)/(\mathbb{K}_\infty \cdot \mathbb{H}_1))) = \mathcal{D}(\mathbb{K}).$$

□

One can also prove constructively that  $\Phi := \mathbb{K}_\infty[E(\mathbb{K})^{1/p^\infty}] \cap \mathbb{H}$  is an unramified extension with group  $A^-(T^*)/(T^*A^-(T^*))$  of rank  $\mathcal{D}(\mathbb{K})$ : for this, one uses  $p$ -adic approximations  $\delta_n \in \overline{E}_1, \delta_n \rightarrow 1$ . The existence of  $\Phi$  and  $A^-[T^*]$  is thus equivalent to the failing of Leopoldt's Conjecture<sup>1</sup>. We call this extension a *phantom* - field and  $A^-[T^*]$  a *phantom module*, for obvious reasons: they encrypt a constant which should be zero.

### 3. PROOF OF THEOREM 1

Following Iwasawa's approach in [9], §9-11, we shall regard the maximal  $p$ -abelian  $p$ -ramified extensions  $\Omega_n/\mathbb{K}_n$  as limits of ray class fields. We start accordingly by reviewing in our context the main results of Takagi theory.

Let  $m$  be a fixed integer and  $N > 0$ ; we consider the  $p$  - parts  $\mathbb{T}_m^{(N)}$  of the ray class fields of  $\mathbb{K}_m$  to the modulus  $(p^N)$ . Then  $\mathbb{H}_m \subset \mathbb{T}_m^{(N)}$ . We have injective sequences with respect to  $m$  and  $N$ :

$$\mathbb{T}_m^{(N)} \subset \mathbb{T}_{m+1}^{(N)} \quad \forall m \geq 0 \quad \text{and} \quad \mathbb{T}_m^{(N)} \subset \mathbb{T}_m^{(N+1)} \quad \forall N \geq 0.$$

We let  $\mathbb{T}_m = \cup_N \mathbb{T}_m^{(N)}$ ; this is by definition the maximal  $p$ -ramified  $p$ -abelian extension of  $\mathbb{K}_m$ , so we have  $\Omega_m = \mathbb{T}_m$ . The galois groups are

$$\mathfrak{X}_m^N = \text{Gal}(\mathbb{T}_m^{(N)}/\mathbb{K}_m), \quad \mathfrak{X}_m = \text{Gal}(\mathbb{T}_m/\mathbb{K}_m) = \text{Gal}(\Omega_m/\mathbb{K}_m).$$

For fixed  $N$  we let  $\mathbb{T}^N = \cup_m \mathbb{T}_m^{(N)}$  and  $\mathfrak{X}^{(N)} = \text{Gal}(\mathbb{T}^{(N)}/\mathbb{K}_\infty)$ . Finally,

$$\Omega = \cup_N \mathbb{T}^{(N)} = \cup_m \mathbb{T}_m = \cup_m \Omega_m, \quad \mathfrak{X} = \text{Gal}(\Omega/\mathbb{K}_\infty).$$

---

<sup>1</sup>The field  $\Phi$  was often noticed in the literature, e.g. in Jaulent's recent paper [11], treating a special case of Leopoldt's Conjecture

We have the projective limits

$$\mathfrak{X}^{(N)} = \varprojlim_m \mathfrak{X}_m^{(N)}, \quad \mathfrak{X}_m = \varprojlim_N \mathfrak{X}_m^{(N)}, \quad \mathfrak{X} = \varprojlim_N \mathfrak{X}^{(N)} = \varprojlim_m \mathfrak{X}_m.$$

We shall use the following expression of the “principal ideal theorem” of Takagi theory (e.g. [10], Chapter V, §6-9):

**Lemma 3.** *Let  $I \subset \mathbb{K}_m$  be an ideal and*

$$x_N = \left( \frac{\mathbb{T}_m^{(N)}/\mathbb{K}_m}{I} \right) \in \mathfrak{X}_m^{(N)}, \quad x = \varprojlim_N x_N \in \mathfrak{X}_m.$$

*Then*

$$(15) \quad x_N = 1 \iff I = (\gamma) \quad \exists e_N \in E_n : \quad e_N \gamma \equiv 1 \pmod{p^N \mathcal{O}(\mathbb{K}_m)},$$

$$(16) \quad x = 1 \iff I = (\gamma) \quad \text{and} \quad 1 \in \gamma \cdot \overline{E}_n.$$

*Proof.* The statement (15) is the usual formulation of the Principal Ideal Theorem of ray class fields. For (16), consider the diagonal embeddings  $\gamma e_N \hookrightarrow \mathbb{K}_n \otimes_{\mathbb{Q}} \mathbb{Q}_p$ . Then  $\lim_{N \rightarrow \infty} \gamma e_N = 1$  and since  $e := \lim_{N \rightarrow \infty} e_N \in \overline{E}_n$ , it follows that  $1 = \gamma e \in \gamma \overline{E}_n$ , as claimed.  $\square$

We assume that  $\mathcal{D}(\mathbb{K}) > 0$ , so  $A^-[T^*]$  is a  $\mathbb{Z}_p$ -module of positive rank  $\mathcal{D}(\mathbb{K})$ . It is a pseudo-cyclical  $\mathbb{Z}_p[\Delta]$ -module, since the radical of  $\Phi$  is pseudo-cyclic. Let thus  $a \in A^-[T^*] \setminus A^p$  be such that  $[A^-[T] : \Lambda[\Delta]a] < \infty$  is minimal and let  $q = p^j$  be the exponent of this module. We shall derive from the assumption  $\mathcal{D}(\mathbb{K}) > 0$  a contradiction, by showing first that  $\mathbf{B}^+$  must be infinite, and then proving that this cannot be the case.

**3.1. A totally unramified  $T$ -extension.** We have seen in the previous section that  $A^-[T^*]$  is a  $\mathbb{Z}_p[\Delta]$ -pseudocyclic module, and thus  $A^-(T^*)$  is  $\Lambda[\Delta]$ -pseudocyclic. Let thus  $a \in A^-(T^*)$  be such that  $\Lambda[\Delta]a$  has finite index in  $A^-(T^*)$  and let  $\mathbb{M}' = \mathbb{K}_{\infty}[A^-(T^*)^{1/p^{\infty}}]$  be the canonic extension defined in the previous chapter. Then  $\mathbb{M} = \mathbb{K}_{\infty}[(\Lambda[\Delta]a)^{1/p^{\infty}}] \subset \mathbb{M}'$  is also a subextension of finite index. But  $A^-$  has no finite  $\Lambda$ -submodules, so infinite galois theory implies  $\mathbb{M} = \mathbb{M}'$ . We shall prove:

**Proposition 3.**

$$\mathbb{M} = \mathbb{K}_{\infty} \left[ A^-(T^*)^{1/p^{\infty}} \right] \subset \mathbb{H}^+.$$

Let  $h = \text{ord}_{T^*}(a) = \text{ord}_{T^*}(A^-) > 0$ , so  $a^{(T^*)^h} = 1$  but  $a^{(T^*)^{h-1}} \neq 1$ . We define the extensions  $\mathbb{F}_i = \mathbb{K}_{\infty}[a^{(T^*)^i \Lambda/p^{\infty}}]$  for  $i = 0, 1, \dots, h-1$ . These are all galois extensions of  $\mathbb{K}$  and  $\mathbb{F}_{i+1} \subset \mathbb{F}_i$  for  $i = 0, 1, \dots, h-2$ . By duality,

$$\text{Gal}(\mathbb{F}_0/\mathbb{K}_{\infty}) \cong (\Lambda a)^{\bullet} \cong \Lambda/(T^h),$$

and the galois group is a cyclic  $\Lambda$ -module. Let thus  $y \in \text{Gal}(\mathbb{F}_0/\mathbb{K}_{\infty})$  be a generator, so  $\text{ord}_T(y) = h$ . We consider the projective Kummer pairing for  $\mathbb{F}/\mathbb{K}_{\infty}$ ; it yields

$$[a^{T^*}, y^{T^{h-1}}]_{\mathbb{F}} = [a^{(T^*)^h}, y]_{\mathbb{F}} = 0,$$

which implies that  $w = y^{T^{h-1}} \in \text{Gal}(\mathbb{F}/\mathbb{K}_\infty)[T]$  fixes  $\mathbb{F}_1 \subset \mathbb{F}_0$ . Let  $\mathbb{L} = \mathbb{K}_\infty[a^{1/p^\infty}] \subset \mathbb{F}_0$ . Then  $\mathbb{F}_0 = \mathbb{F}_1 \cdot \mathbb{L}$ ; since  $w \neq 1$  fixes  $\mathbb{F}_1$  and  $\mathbb{L}/\mathbb{K}_\infty$  is a  $\mathbb{Z}_p$ -extension, it follows that  $w|_{\mathbb{L}}$  is a generator of  $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ . Indeed, it acts non trivially on  $\mathbb{L}$  and if it is not a generator of the galois group, then there is a  $w' \in [y^{T^i} : 0 \leq i < h-1]_{\mathbb{Z}_p}$  which generates this group. One can prove by induction that  $\text{Gal}(\mathbb{F}_1/\mathbb{K}_\infty) = [y^{T^i} : 0 \leq i < h-1]_{\mathbb{Z}_p}$  and this would imply  $\mathbb{Z}_p\text{-rk}(\text{Gal}(\mathbb{F}_0/\mathbb{K}_\infty)) = h-1 < \mathbb{Z}_p\text{-rk}(\text{C-Rad}(\mathbb{F}_0/\mathbb{K}_\infty))$ , which is absurd. Therefore  $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty) = w^{\mathbb{Z}_p}$ .

We claim also that  $\mathbb{M} \subset \mathbb{H}$  iff  $\mathbb{L} \subset \mathbb{H}$ . If  $\mathbb{L} \not\subset \mathbb{H}$ , a fortiori  $\mathbb{M} \not\subset \mathbb{H}$ . Conversely, if  $\mathbb{L} = \mathbb{K}_\infty[a^{1/p^\infty}] \subset \mathbb{H}$ , we note that  $\mathbb{M}' = \mathbb{K}_\infty[a^{\Delta/p^\infty}]$  is the galois closure of  $\mathbb{L}$  over  $\mathbb{Q}$ . Since  $\mathbb{L} \subset \mathbb{H}$  and  $\mathbb{H}$  is also galois over  $\mathbb{Q}$ , while the galois closure is the smallest galois extension of  $\mathbb{Q}$  containing  $\mathbb{L}$ , it follows a fortiori that  $\mathbb{M}' \subset \mathbb{H}$ . Since we have shown that  $\mathbb{M}' = \mathbb{M}$ , it follows that  $\mathbb{K}_\infty[(A^-(T^*))^{1/p^\infty}] \subset \mathbb{H}$ . We have thus proved:

**Lemma 4.** *Notations being like above, let  $\mathbb{L} = \mathbb{K}_\infty[a^{1/p^\infty}]$  and  $\mathbb{F}_0 = \mathbb{K}_\infty[a^\Delta/p^\infty]$ . Then there is a  $w \in \text{Gal}(\mathbb{F}_0/\mathbb{K}_\infty)[T]$  which generates  $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$  by restriction. Moreover  $\mathbb{M} \subset \mathbb{H}$  if and only if  $\mathbb{L} \subset \mathbb{H}$ .*

We shall also need the following auxiliary result:

**Lemma 5.** *Let  $c \in \mathbb{K}^\times$  with  $c \equiv 1 \pmod{\wp}$  for all  $\mathcal{O}(\mathbb{K}) \supset \wp \supset (p)$  and  $N > 0$  be a fixed integer. Then there is an  $n_1 > 0$  such that for all  $n > n_1$  we have*

$$(17) \quad c^{p^{n-k}} \equiv 1 \pmod{p^N \mathcal{O}(\mathbb{K})}$$

*Proof.* We prove the claim locally for every completion. Let thus  $c' \in \mathbb{K}_\wp$  be the image of  $c$  in the completion at a prime  $\wp \subset \mathbb{K}$  above  $p$  and let  $\pi \in \mathbb{K}_\wp$  be a uniformizer, let  $e(\mathbb{K})$  be the ramification index of  $p$  in  $\mathbb{K}$  and thus in  $\mathbb{K}_\wp$ . We assumed that  $v_p(c' - 1) > 0$ , so  $c' = 1 + d\pi$ ,  $d \in \mathbb{K}_\wp$  and for  $m > 0$ ,

$$(c')^{p^m} = (1 + d\pi)^{p^m} = 1 + \sum_{i=1}^{p^m} \binom{p^m}{i} \pi^i.$$

From the divisibility of the binomial coefficients by powers of  $p$ , we see that for  $e(\mathbb{K}) > 1$  we have  $\min v_p \left( \binom{p^m}{i} \pi^i \right) = v_p(\pi^{p^m}) = p^m/e(\mathbb{K})$ . For  $e(\mathbb{K}) = 1$ , the minimum is  $p^m$ ; in both cases it diverges with  $m \rightarrow \infty$  and thus, for sufficiently large  $n$  we may achieve that  $((c')^{p^{n-k}} - 1) \in p^N U(\mathbb{K}_\wp)$  for all primes  $\mathbb{K} \supset \wp \supset (p)$ . Consequently  $c^{p^{n-k}} \equiv 1 \pmod{p^N \mathcal{O}(\mathbb{K})}$  uniformly, for sufficiently large  $n$ .  $\square$

We now prove the main result of this section:

**Lemma 6.** *Let  $a \in A^-(T^*)$  be a generator of this module as a pseudocyclic  $\Lambda[\Delta]$ -module and  $\mathbb{L} = \mathbb{K}_\infty[b^{1/p^\infty}]$ . Then  $\mathbb{L} \subset \mathbb{H}$ .*

*Proof.* Suppose that the claim is false, so  $\mathbb{L} \cap \mathbb{H} = \mathbf{K}$  with  $[\mathbf{K} : \mathbb{K}_\infty] = p^u < \infty$ . Let  $\mathbf{K}_n = \mathbb{H}_n \cap \mathbb{L}$ ; we may assume that the base field  $\mathbb{K}$  is chosen such

that  $[\mathbf{K}_1 : \mathbb{K}] = p^u$ , so  $[\mathbf{K}_n : \mathbb{K}_n] = p^u$  for all  $n$ . Since  $\mathbb{F}_0$  is the galois closure of  $\mathbb{L}$  over  $\mathbb{K}$ , we may then choose a lift  $\tilde{\Gamma} \in \text{Gal}(\mathbb{F}_0/\mathbb{K})$  such that its action on  $\mathbf{K}$  by restriction fixes  $\mathbf{K}_1$ . Let  $\mathbb{L}_1 = \mathbb{L}^{\tilde{\Gamma}} \supset \mathbf{K}_1$  and  $\mathbb{L}_n = \mathbb{L}_1 \cdot \mathbb{K}_n \subset \mathbf{K}_n$ .

We have shown in Lemma 4 that there is a  $w \in \text{Gal}(\mathbb{F}_0/\mathbb{K}_\infty)[T]$  which generates  $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$  by restriction. We show that there is a lift  $x \in X := \text{Gal}(\Omega^+/\Omega_{E'})[T]$  of  $w$ . Let  $F(T) = T^h g(T)$  be the minimal annihilator polynomial of  $X$  and  $\mathbb{M}_g = \mathbb{K}_\infty[(A^-(g))^{1/p^\infty}]$ . Then  $\Omega = \mathbb{M}_g \cdot \mathbb{M}$  and  $[\mathbb{M} \cap \mathbb{M}_g : \mathbb{K}_\infty] < \infty$ . Consequently, the generator  $y \in \text{Gal}(\mathbb{F}_0/\mathbb{K}_\infty)$  defined before Lemma 4 lifts to some  $x' \in X(T)$  and letting  $x = (x')^{T^{h-1}}$  we have  $x \in X[T]$  and  $x|_{\mathbb{L}} = y^{T^{h-1}}|_{\mathbb{L}}$  is a generator of  $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ .

Let now  $n > k$  and  $\mathbb{T}_n^{(N)}$  be the ray class field defined for an  $N$  such that  $\mathbf{K}_n \subsetneq \mathbb{L}_n \cap \mathbb{T}_n^{(N)}$  and let  $x_n^{(N)} = x|_{\mathbb{T}_n^{(N)}} \in \mathfrak{X}_n^{(N)}[T] = \text{Gal}(\mathbb{T}_n^{(N)}/\mathbb{K}_n)[T]$ . Then  $(x_n^{(N)})^{p^u}$  fixes  $\mathbb{H}_n$  and generates  $\text{Gal}((\mathbb{L}_n \cap \mathbb{T}_n^{(N)})/\mathbf{K}_n)$ . Furthermore, the sequence  $(x_n^{(N)})_{N \in \mathbb{N}}$  is projective with limit  $x_n \in \mathfrak{X}_n[T]$ . By Tchebotarew's Theorem, there is a prime  $\mathfrak{q} \subset \mathcal{O}(\mathbb{K}_n)$  which is totally split in  $\mathbb{K}_n/\mathbb{Q}$  and coprime to  $p$ , such that  $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{q}}\right) = (x_n^{(N)})^{p^u}$ . Let  $\mathfrak{q}_1 = N_{n,1}(\mathfrak{q})$  be the prime of  $\mathbb{K}$  below  $\mathfrak{q}$ . Since  $\mathfrak{q}$  is totally split, the action of  $x_n$  by restriction to  $\mathbb{L}_1 \cap \mathbb{T}_n^{(N)}$  implies for all  $N$  that

$$\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{q}}\right)\Big|_{\mathbb{L}_1} = \left(\frac{(\mathbb{L}_1 \cap \mathbb{T}_1^{(N)})/\mathbf{K}_1}{\mathfrak{q}_1}\right).$$

We may choose  $N$  sufficiently large, so that  $\mathfrak{q}_1$  is inert in some non trivial extension  $\mathbf{K}_1 \subset \mathbf{L} \subset \mathbb{L}_1$ . Since  $\mathbb{L}_1/\mathbf{K}_1$  is cyclic, it follows that  $\mathfrak{q}_1$  is inert in  $\mathbb{L}_1/\mathbf{K}_1$ . We shall derive a contradiction to this fact, which shows that  $\mathbb{L} \subset \mathbb{H}$ .

By choice of  $x_n^{p^u}$ , the prime  $\mathfrak{q}$  fixes  $\mathbb{H}_n$ , so it must be principal:  $\mathfrak{q} = (\gamma), \gamma \in \mathcal{O}(\mathbb{K}_n)$ . Since  $x_n^{(N)} \in \mathfrak{X}_n^{(N)}[T]$ , we have  $(x_n^{(N)})^T = 1$  and a fortiori  $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\mathfrak{q}^T}\right) = 1$ . The Lemma 3 implies that  $1 \in \gamma^T \cdot \overline{E}(\mathbb{K}_n)$ , so  $\gamma^T \in \overline{E}(\mathbb{K}_n)$ .

It follows that  $\gamma = c \cdot e$  with  $c \in U(\mathbb{K}), e \in \overline{E}_n$ . But then  $\gamma_1 = N_{n,1}(\gamma) = c^{p^{n-k}} \cdot N_{n,1}(e)$ . By raising  $\gamma$  to some power coprime to  $p$ , we may assume that  $c \equiv 1 \pmod{\wp}$  for all primes  $\wp \supset (p)$  of  $\mathbb{K}_n$ . We may thus apply the Lemma 5 and see that for fixed, large  $N$  and some  $n$  depending on  $N$  using the result of the lemma, we have  $\gamma_1 \in \overline{E}(\mathbb{K}_1) \cdot U(\mathbb{K}_1)^{p^N}$ . Takagi theory implies then that

$$y_1 := \left(\frac{\mathbb{T}_1^{(N)}/\mathbb{K}}{(\gamma_1)}\right) = \left(\frac{\mathbb{T}_1^{(N)}/\mathbb{K}}{\mathfrak{q}_1}\right) = 1.$$

This contradicts the fact that  $(\mathbb{T}_1^{(N)} \cap \mathbb{L}_1)/\mathbf{K}_1$  is a non trivial cyclic extension, in which the primes above  $\mathfrak{q}_1$  are inert. The assumption that  $\mathbf{K} = \mathbb{L} \cap \mathbb{H}$  is



a finite extension of  $\mathbb{K}_\infty$  must thus be false and  $\mathbb{L} \subset \mathbb{H}$ . This completes the proof of the lemma.  $\square$

Proposition 3 follows from Lemmata 4 and 6, as explained above. Our next result is

**Lemma 7.**

$$[\Omega_{E'}[(A^+[T])^{1/p^\infty}] \cap \overline{\mathbb{H}} : \Omega_{E'}] < \infty.$$

*Proof.* Assuming that the claim is false, there is at least one  $b \in A^+[T]$  such that  $\Omega_{E'}[b^{1/p^\infty}] \subset \overline{\mathbb{H}}$ . After eventually replacing  $a$  by  $a^t$  for some  $t \in \mathbb{Z}_p[\Delta]$ , we may assume that  $\varphi(b)$  generates by restriction  $\text{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ , with  $\mathbb{L} = \mathbb{K}_\infty[a^{1/p^\infty}]$ . We shall use Takagi theory and show that  $\ell(b)$  is finite. Then

$$(18) \quad A^+[T] = \mathbf{B}^+$$

follows from (14). We fix  $n > k$  and recall that by the choice of the base field  $\mathbb{K}$  in the introduction, the class lift map  $\iota_{n,n+1} : A_n \rightarrow A_{n+1}$  is injective on  $\Lambda b = \mathbb{Z}_p b$  for all  $n \geq 0$  and  $\text{ord}(b_n) = p^{n+z(b)}$  for all  $n$  and  $z(b) \leq z$ . Note also the identity in the group ring:

$$(19) \quad N_{n,1} = p^{n-k} + Tw = p^{n-k} \left( 1 + \frac{p^{n-k} - 1}{2} T \right) + T^2 w_1,$$

for  $w, w_1 \in \mathbb{Z}[T]$ . Let  $\mathfrak{Q} \in b_n$  be a totally split prime above  $\mathbb{Q}$  which is coprime to  $p$ . Then  $\mathfrak{Q}^T = (\nu)$  is principal and  $N_{n,1}(\nu) \in E(\mathbb{K})$ . From (19) we deduce that the prime in  $\mathbb{K}$  below  $\mathfrak{Q}$  verifies

$$\mathfrak{q} = N_{n,1}(\mathfrak{Q}) = \mathfrak{Q}^{p^{n-k}} \cdot (\nu^w).$$

By raising this identity to the power  $q := p^{n+z(b)}/p^{n-k} = \text{ord}(b_1)$ , an equality which follows from the stability of the transitions in  $\Lambda b$ , we find

$$(\alpha_1) = \mathfrak{q}^{\text{ord}(b_1)} = \mathfrak{Q}^{p^{n+z(b)}} \cdot (\nu^{qw}).$$

If  $(\alpha_n) = \mathfrak{Q}^{p^{n+z(b)}}$ , the previous identity yields

$$(20) \quad \delta \alpha_n = \alpha_1 \cdot \nu^{-qw}, \quad \delta \in E(\mathbb{K}_n).$$

Since  $b$  is a real class,  $\ell(b_n) = [\Omega_{E'}[b_n^{1/p^\infty}] \cap \overline{\mathbb{H}} : \Omega_{E'}]$  and we may consider  $\alpha_n, \nu \in \Omega_{E'}$ , so the units of  $\mathbb{K}_n$  are  $p$ -powers and (20) becomes:

$$(21) \quad \alpha_n^T = \nu^{-wqT}$$

Let now  $N > 0$  be fixed and consider the fields  $\mathbb{T}^{(N)} \supset \mathbb{H}^+ \supset \mathbb{M} \supset \mathbb{L}$  defined above. Let  $\varphi(b) \in \text{Gal}(\mathbb{H}^+/\mathbb{K}_\infty)$  be the image of the Artin map, which restricts to  $y$ , and let  $x = (x_n)_{n \in \mathbb{N}} \in \mathfrak{X}^{(N)}[T]$  be a lift of  $\varphi(b)$ , with  $x_n \in \mathfrak{X}_n^{(N)}$ . We assume that  $\mathfrak{Q}$  is chosen, by using Tchebotarew, such that

$\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\Omega}\right) = x_n$ . Then

$$1 = x_n^T = \left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\Omega^T}\right) = \left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{(\nu)}\right),$$

and Lemma 3 implies that there is a unit  $e_N \in E_n$  with  $\nu e_N \equiv 1 \pmod{p^N}$ . It follows that, modulo units,  $\nu$  can be chosen to be locally arbitrarily small:  $1 \in \nu \overline{E}_n$  and (21) yields  $\alpha_n^T \in \overline{E}_n^{qT}$ , so  $\alpha_n \in U(\mathbb{K}) \cdot \overline{E}_n^q$ . There is a  $c_1(n) \in U(\mathbb{K})$  such that  $\alpha_n/c_1(n) \in \overline{E}_n^q$  and (20) implies

$$(22) \quad \Omega_{E'}[b_n^{1/p^{n+z(b)}}] = \Omega_{E'}[\alpha_n^{1/p^{n+z(b)}}] = \Omega_{E'}[c_1(n)^{1/p^{n+z(b)}}].$$

We shall show that this extension has bounded intersection with  $\overline{\mathbb{H}}$ . Let  $\tilde{\Gamma} \subset \text{Gal}(\mathbb{M}/\mathbb{K}_\infty)$  be a lift of  $\Gamma$  which fixes  $\mathbf{K}_1 := \mathbb{L} \cap \mathbb{H}_1$  and let  $\mathbb{L}_1 = \mathbb{L}^{\tilde{\Gamma}}$ . The Artin symbol  $\varphi(b_1) = \left(\frac{\mathbb{H}_1/\mathbb{K}}{\mathfrak{q}}\right) \neq 1$  and thus  $\mathfrak{q}$  is inert in  $\mathbf{K}_1/\mathbb{K}$ . Since  $\mathbb{L}_1 \supset \mathbf{K}_1 \supset \mathbb{K}$  is a  $\mathbb{Z}_p$ -extension, it follows that  $\mathfrak{q}$  is inert in  $\mathbb{L}_1$  and  $x_1 = \left(\frac{\mathbb{L}_1/\mathbb{K}}{\mathfrak{q}}\right) \in \text{Gal}(\mathbb{L}_1/\mathbb{K})$  generates this group. But then

$$\mathbb{Z}_p \left(\frac{\mathbb{L}_1/\mathbb{K}}{(\alpha_1)}\right) = \mathbb{Z}_p x_1^{\text{ord}(\alpha_1)} = (\text{Gal}(\mathbb{L}_1/\mathbb{K}))^{\text{ord}(\alpha_1)} = \text{Gal}(\mathbb{L}_1/\mathbf{K}_1).$$

Let  $l \geq 0$  be minimal such that  $\mathbb{T}_1^{(l)} \cap \mathbb{L}_1 \not\supset \mathbf{K}_1$ . Then  $\left(\frac{\mathbb{T}_1^{(N)}/\mathbf{K}_1}{(\alpha_1)}\right) \neq 1$  for  $N \geq l$ . In particular, Lemma 3 shows that there is a maximal  $l' \geq 0$  with  $\alpha_1 \overline{E}(\mathbb{K}) \cap U(\mathbb{K})^{p^{l'}} \neq \emptyset$  and  $l'$  does not depend on  $n$ , but only on  $\mathbb{L}_1$  and  $\alpha_1$ . In view of (22), it follows that  $c_1 \notin \overline{E}(\mathbb{K})U(\mathbb{K})^{p^{l'+1}}$ . Since  $c_1 \in \alpha_n \cdot \overline{E}_n^q$ , we conclude that  $\ell(a_n) \leq l'$  and thus  $\ell(a) < \infty$ , which completes the proof of the Lemma 7  $\square$

We now give the proof of Lemma 1, which is similar to the proof of Lemma 7:

*Proof.* We now consider  $\mathbb{L} = \mathbb{K}_\infty[a^{T^*/p^\infty}]$ , a field in which  $w' = y^{T^{h-2}}$  generates the galois group. In particular, if  $h > 1$  then  $w' = \varphi(b)$  for some  $b \in (A')^+[T]$ . We follow the proof of Lemma 7 and choose a lift  $x \in X[T^2]$  of  $\varphi(b)$ ; for fixed  $n > k$  and large  $N$  we choose  $\Omega \subset \mathbb{K}_n$  a totally split prime with  $\left(\frac{\mathbb{T}_n^{(N)}/\mathbb{K}_n}{\Omega}\right) = x|_{\mathbb{T}_n^{(N)}}$ . We have

$$\begin{aligned} \Omega &= (\nu) \cdot \mathfrak{P}, \quad [\mathfrak{P}] \in \mathbf{B}_n, \quad \mathfrak{P} \cap \mathbb{Z} \subseteq (p), \\ \mathfrak{q} &= \Omega^{p^{n-k}} \cdot \mathfrak{P}^{p^{n-k}(1+dT+O(T^2))} \cdot (\nu^w) \\ &= \Omega^{p^{n-k}} \cdot \mathfrak{P}_1 \cdot (\nu^w), \end{aligned}$$

where  $\mathfrak{P}_1 = \mathfrak{P}^{n-k} = N_{n,1}(\mathfrak{P}) \subset \mathbb{K}$ . Raising to the power  $q = p^{z(b)-k} = \text{ord}(b_1)$  we obtain

$$(\alpha_1) = \Omega^{p^{n+z(b)}} \cdot \mathfrak{P}_1^q \cdot (\nu^{qw}),$$

and eventually, over  $\Omega_{E'}$ :

$$(23) \quad \begin{aligned} \alpha_n &= \alpha_1 \cdot \Pi_1 \cdot \nu^{-qw}, \quad \Pi_1 \in E'(\mathbb{K}), \quad \text{hence} \\ \alpha_n^T &= \nu^{-qwT}. \end{aligned}$$

Using the same argument as in the previous proof, and since only  $T^2$  annihilates  $x$ , we obtain this time  $\nu^T \in E_n \cdot (\mathbb{K}_n^\times)^{p^N}$ , and for  $N \rightarrow \infty$ , also  $\nu^T \in \overline{E}_n$ . If  $\nu \in \overline{E}_n$ , the argument may be concluded like in the previous proof. Suppose that  $\nu^T \in E_n \cdot (\mathbb{K}_n^\times)^{p^N}$ , say  $\nu^T = e \cdot x^{p^N}$ ; then  $N_{n,1}(e) = N_{n,1}(x)^{-p^N}$  and thus  $N_{n,1}(x) \in E(\mathbb{K})$ , so  $(x) = \mathfrak{B}^T$  and taking  $N$  sufficiently large with respect to the order  $p^m = \text{ord}(\mathfrak{B})$ , we find  $x = \delta \cdot \beta^{p^{N-m}T}$ , so  $(\nu/\beta^{p^{N-m}})^T = e' \in E(\mathbb{K}_n)$ . Then  $(\nu/\beta^{p^{N-m}})$  is the lift of an ideal from  $\mathbb{K}_1$  that capitulates. Since the exponent of the finite torsion of  $A^+$  is bounded, there is an  $m \geq k$  such that all primes from  $\mathbb{K}_1$  which capitulate in  $\mathbb{K}_\infty$  are already principal in  $\mathbb{K}_m$ . In this case,  $\nu \in \mathbb{K}_m^\times \cdot E_n \cdot (\mathbb{K}_n^\times)^{p^{N-m}}$ ; since  $m$  is fixed, the proof can be completed with a slight modification, in this case too, thus confirming the claim of the lemma.  $\square$

As a consequence, we have

**Corollary 1.** *Notations being like above*

$$\mathbb{Z}_p\text{-rk}(A^-[T^*]) = \mathcal{D}(\mathbb{K}) \quad \text{and} \quad A^+(T) \sim \mathbf{B}^+ \cong (A^-(T^*))^\bullet.$$

If  $F(T^*)$  is the minimal annihilator polynomial of  $A^-$ , then  $F(T^*) = T^* \cdot G(T^*)$  with  $G(0) \neq 0$ .

*Proof.* From Lemmata 1 and 7 we conclude that  $A^+(T) = \mathbf{B}^+$ . By reflection, it follows that  $\text{ord}_{T^*}(A^-(T^*)) = 1$  and  $A^-(T^*) = A^-[T^*]$ . Finally,

$$A^+[T] \sim \mathbf{B}^+ = \text{Gal}(\overline{\mathbb{L}}/\mathbb{K}_\infty) \cong (A^-[T^*])^\bullet.$$

The fact that  $F(T^*)$  is not divisible by  $(T^*)^2$  is a reformulation of  $A^-(T) = A^-[T]$ .  $\square$

**3.2. The finiteness of  $\mathbf{B}^+$ .** We prove in this section

**Theorem 2.** *The module  $\mathbf{B}^+$  is finite.*

We recall that the systems  $E_n, U'_n = \{u \in U^{(1)}(\mathbb{K}_n^+) : N_{\mathbb{K}_n/\mathbb{Q}}(u) = 1\}$ ,  $\overline{E}_n$  are projective with respect to the norms and the norms are even surjective for  $(U'_n)_{n \in \mathbb{N}}$ . We let thus  $E_\infty = \varprojlim_n E_n, U'_\infty = \varprojlim_n U'_n$  and  $\overline{E}_\infty = \varprojlim_n \overline{E}_n = \overline{E_\infty}$ .

In addition, for  $X \in \{E, U, \overline{E}\}$ , we define

$$X_{n,H} = \{x \in X_n : N_{n,1}(x) = 1\}, \quad X_{\infty,H} = \varprojlim_n X_{n,H}.$$

Since we have assumed that the Leopoldt defect is stationary for all  $\mathbb{K}_n$ , we have  $\mathbb{Z}_p\text{-rk}(\overline{E}_{n,H}) = \mathbb{Z}_p\text{-rk}(U_{n,H})$  for all  $n$ . We let  $D = \Delta^+ = \text{Gal}(\mathbb{K}^+/\mathbb{Q})$  and  $R = \mathbb{Z}_p[\Delta]$ ; then  $\mathbb{Z}_p\text{-rk}(R) = r_2 = |D|$ . Fixing a lift  $\tilde{\Delta} \subset \text{Gal}(\mathbb{K}_\infty/\mathbb{Q})$  of  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ , the module  $R$  acts on all  $\mathbb{Z}_p$ -modules attached to  $\mathbb{K}_\infty$ . Let

$\mathbb{L}_n = \mathbb{M} \cdot \mathbb{H}_n^+ = \Omega(\mathbb{K}^+) \cdot \mathbb{H}_n^+$  be the maximal abelian extension of  $\mathbb{K}_n^+$  contained in  $\Omega^+$  and  $Y_n = \text{Gal}(\Omega_n^+/\mathbb{L}_n)$ . The modules  $U_{n,H}, \overline{E}_{n,H}$  are related to the galois groups and their annihilators by

**Lemma 8.** *Notations being like above, let*

$$Y := \text{Gal}(\Omega^+ / (\mathbb{H}^+ \cdot \Omega_1)) = \text{Gal}(\Omega^+ / \mathbb{H}^+) \cong U_{\infty,H} / \overline{E}_{\infty,H}.$$

*Then  $Y$  is a module annihilated by  $G(T)$  and for all  $n$  sufficiently large we have*

$$U_{n,H}^{G(0)} \subset \overline{E}_{n,H} \cdot U_n^T.$$

*Proof.* From Proposition 3 we deduce that  $\Omega(\mathbb{K}^+) = \mathbb{L}_1 = \mathbb{M} \cdot \mathbb{H}_1^+ \subset \mathbb{H}^+$ . We have for all  $n > k$ , by class field theory,

$$\text{Gal}(\Omega_n^+ / (\overline{\mathbb{H}} \cap \Omega_n^+)) \cong U_n^+ / \overline{E}_n,$$

via the global Artin map  $\varphi$ . Artin acts by restriction of  $\mathbb{L}_1$  and  $\varphi(U_n')|_{\mathbb{L}_n} = \varphi(U_1')$ . Hence  $\text{Gal}(\Omega_n^+ / \mathbb{L}_n) = \varphi(U_n' / (U_1' \cdot \overline{E}_n))$ . We have the following decompositions as direct products:  $U_n' = U_1' \cdot U_{n,H}$  and  $U_1' \cdot \overline{E}_n = U_1' \cdot \overline{E}_{n,H}$ , with  $\{1\} = U_1' \cap U_{n,H} \supseteq U_1' \cap \overline{E}_{n,H}$ . Thus

$$U_n' / (U_1' \cdot \overline{E}_n) = (U_1' \cdot U_{n,H}) / (U_1' \cdot \overline{E}_{n,H}) = U_{n,H} / \overline{E}_{n,H},$$

and the Artin map induces an isomorphism

$$(24) \quad \text{Gal}(\Omega_n^+ / \mathbb{L}_n) \cong U_{n,H} / \overline{E}_{n,H}, \quad \text{Gal}(\Omega^+ / \mathbb{H}^+) \cong U_{\infty,H} / \overline{E}_{\infty,H}.$$

We see from Corollary 1 that the minimal annihilator polynomial of  $\text{Gal}(\Omega^+ / \mathbb{M})$  is  $G(T)$  with  $G(0) \neq 0$ . Then (24) implies that  $G(T)$  is a fortiori an annihilator of  $U_{\infty,H} / \overline{E}_{\infty,H}$ . Therefore

$$U_{\infty,H}^{G(0)} \cdot U_{\infty}^{Th(T)} \subset \overline{E}_{\infty,H},$$

with  $G(T) = G(0) + Th(T)$ ; thus

$$(25) \quad U_{\infty,H}^{G(0)} \subset \overline{E}_{\infty,H} \cdot U_{\infty,H}^T.$$

The relation holds for  $n$  sufficiently large, and this completes the proof of the lemma.  $\square$

The next lemma relates  $E_{n,H}$  to the  $p$ -units:

**Lemma 9.** *Notations being like above, if  $p^m$  is the exponent of  $A_1$ , then for sufficiently large  $n$ , we have*

$$(26) \quad E_{n,H}^{p^m} \subset (E_n')^T \quad \text{and} \quad \overline{E}_{n,H}^{p^m} \subset (\overline{E}_n')^T.$$

*Proof.* We have  $E_n \supset (E_n')^T \supset E_n^T$ , since  $E_n \subset E_n'$  and for  $\rho \in E_n'$ , the ideal  $(\rho)^T = (\prod_{\nu \in C^+} \wp_n^{c_\nu}) = (1)$ , so  $\rho^T \in E_n$ . Let now  $\delta \in E_{n,H} \setminus E_n^T$ . By definition, we have  $N_{n,1}(\delta) = 1$  and thus  $\delta = \gamma^T$  for some  $\gamma \in \mathbb{K}_n$ , by Hilbert 90. Then  $(\gamma) = \mathfrak{A}$  for some ambig ideal; let  $m'$  be the smallest

integer, such that all the prime ideals in classes of  $A'_1$  which capitulate in  $\mathbb{K}_n$  for sufficiently large  $n$ , already capitulate in  $A_{m'}$ . It follows that

$$\begin{aligned}\gamma &= \beta_{m'} \cdot \rho, \quad \beta_{m'} \in \mathbb{K}_{m'}, \quad \rho \in E'_n, \quad \text{hence} \\ \delta &= \gamma^T = \beta_{m'}^T \cdot \rho^T \in E_{m',H} \cdot (E'_n)^T.\end{aligned}$$

Since  $(\beta_{m'}) = \mathfrak{A}\mathcal{O}(\mathbb{K}_{m'})$  for some  $\mathfrak{A} \in a \in A'_1$ , it follows from the choice of  $m$  that  $\mathfrak{A}^{p^m} = (\alpha_1)$  is a principal ideal of  $\mathbb{K}$ , so  $\alpha_1 \in \mathbb{K}$  and  $\beta_{m'}^{p^m} \in \alpha_1 \cdot E_{m'}$  and  $\delta^{p^m} \in E_{m',H}^T \cdot (E'_n)^T$ . This holds for any  $\delta \in E_{n,H}$ , so  $E_{n,H}^{p^m} \subset (E'_n)^T$ , which is the claim of (26).

Passing to  $p$ -adic completions, let  $d \in \overline{E}_{n,H}$ ; for arbitrary large  $N$ , there are then units  $\delta_N \in E_{n,H}$  such that  $d \in \delta_N U_n^{p^N}$  and thus

$$d^{p^m} \in \delta_N^{p^m} U_n^{p^{N+m}} \subset (E'_n)^T U_n^{p^{N+m}}.$$

Therefore  $d^{p^m} \in \bigcap_N (E'_n)^T \cdot U_n^{p^N} = (\overline{E}'_n)^T$ , which completes the proof.  $\square$

We can now complete the proof of Theorems 2 and 1:

*Proof.* By combining (25) with (26) we obtain

$$(27) \quad U_{n,H}^{G(0)p^m} \subset \left( \overline{E}' \cdot U'_n \right)^T.$$

Let  $p^z$  be the exponent of  $A_1$ , so  $p^{z+n-k}$  annihilates  $A_n$ . We shall show that this implies that  $p^{m+z}G(0)$  annihilates  $\mathbf{B}_n^+$ , and since the exponent does not depend on  $n$ , this will confirm the fact that  $\mathbf{B}^+$  is finite and thus  $\mathcal{D}(\mathbb{K}) = 0$ .

Let  $\wp \subset P^+$  be a prime of  $\mathbb{K}^+$  above  $p$  and  $\mathbb{K}_{\wp,\infty}/\mathbb{K}_{wp}$  the cyclotomic ramified  $\mathbb{Z}_p$ -extension of the completion of  $\mathbb{K}$  at  $\wp$ . We write  $\tau$  for a topological generator of  $\Gamma = \text{Gal}(\mathbb{K}_{\wp,\infty}/\mathbb{K}_{wp})$  and consider a uniformizer  $\pi_n \in \mathbb{K}_{n,\wp}$ , the  $n$ -th level subextension of  $\mathbb{K}_{\infty,\wp}$ . Since  $\wp$  is totally ramified, we have  $\pi_n^{p^{n-k}} = \pi \in \mathbb{K}_{\wp}$ , a uniformizer of  $\mathbb{K}$ . The ramification index being exactly  $p^{n-k}$ , it follows also that  $\pi_n^{p^{n-k}} \notin \mathbb{K}_{\wp}$ . Let  $e_n = \pi_n^T \in \iota_{\wp}(U_{n,H})$ . Then  $e_n$  has order  $p^{n-k}$  in  $\iota_{\wp}(U_{n,H})/U_{n,\wp}^T$ . Suppose that  $e_n^{p^j} \in U_{n,\wp}^T$  for some  $j > 0$ . Then there is an  $x \in U_{n,\wp}$  such that  $(\pi_n^{p^j}/x)^T = 1$  and thus  $\pi_n^{p^j} = x \cdot u_1, u_1 \in U_{1,\wp}$ . The canonic valuation  $v_p : \mathbb{C}_p \rightarrow \mathbb{R}$  is then

$$p^j v_p(\pi_n) = p^j / p^{n-k} v_p(\pi) = p^{k+j-n} v_p(\pi) = v_p(u_1 x) \geq v_p(\pi),$$

since  $x$  is a unit and thus  $u_1$  must be divisible by some power of  $\pi$ ; therefore  $j \geq n - k$  and consequently  $\overline{e}_n \in \iota_{\wp}(U_{\wp,H})/U_{n,\wp}^T$  has order  $p^{n-k}$ .

We may choose  $u \in U_{n,H}$  such that  $\iota_{\wp}(u) = e_n^{p^{2m}G(0)}$  and  $\iota_{\nu\wp} = 1$  for all  $\nu \in C^+ \setminus \{1\}$ . By (27), we have  $y := u^{p^{2m}G(0)} \in (\overline{E}' \cdot U_n)^{p^m T}$ . Let  $n$  be such that  $p^{n-k} > p^{2m}G(0)$ . Then  $y \notin (U_n)^T$  so  $y = \rho^{p^m T} \cdot x^T, x \in U_n^{p^m}$  and  $1 \neq \rho \in \overline{E}'$ . Let  $\rho_{\nu\wp} = \iota_{\nu\wp}(\rho)$ . Then  $(\rho_{\wp} x_{\wp} / \pi_n^{p^m G(0)})^T = 1$ , hence

$\rho_\wp = \pi_n^{p^m G(0)} \cdot y_1/x_\wp$ , with  $y_1 \in \mathbb{K}_\wp$ . Then  $v_p(y_1)/v_p(\pi_n) \equiv 0 \pmod{p^{n-k}}$  and since  $x$  is a unit, it follows that

$$\begin{aligned} v_p\left(\rho_\wp/\pi_n^{p^m G(0)}\right)/v_p(\pi_n) &\equiv 0 \pmod{p^{n-k}}, \quad \text{hence} \\ v_p(\rho_\wp)/v_p(\pi_1) &\equiv p^m G(0) \pmod{p^{n-k}} \end{aligned}$$

There is a sequence of  $p$ -units  $\rho_N \in E'_n \cap \mathcal{O}(\mathbb{K}_n)$  approximating  $\rho$  by  $\rho = \rho_N u_N^{p^{2N}}$ ,  $u_N \in U_n$ .

$$(28) \quad v_p(\iota_{\nu\wp}(\rho_N))/v_p(\pi_n) \equiv \begin{cases} 0 \pmod{p^{n-k}} & \text{for } \nu \neq 1, \text{ and} \\ p^m G(0) \pmod{p^{n-k}} & \text{for } \nu = 1. \end{cases}$$

Let  $(\rho_N) = \prod_{\nu \in C^+} \wp_n^{c_\nu \nu}$  be the prime decomposition of  $\rho_N$ . By comparing valuations, we see that  $c_\nu = v_p(\iota_{\nu\wp}(\rho_N))/v_p(\pi_n)$ , and the previous conditions imply  $c_\nu \equiv 0 \pmod{p^{n-k}}$  for  $\nu \neq 1$  and  $c_1 \equiv p^m G(0) \pmod{p^{n-k}}$ . We deduce from the fact that  $p^m$  annihilates  $A_1$  and the choice of  $\mathbb{K}$  such that (3) holds in cyclic  $\Lambda$ -modules of infinite orders for all  $n \geq k$ , that  $p^{m+n-k}$  annihilates  $\mathbf{B}_n^+$ . Since  $c_\nu \equiv 0 \pmod{p^{n-k}}$  for all  $\nu \neq 1$ , we see that  $(\nu\wp)^{p^m c_\nu} = (r_\nu)$  are principal ideals, with  $r_\nu \in E'_n$ . It follows that

$$(\rho_N^{p^m}) = \wp^{c_1} \cdot \left( \prod_{\nu \neq 1} r_\nu \right).$$

Moreover, we gather from (28) that  $c_1 = p^m G(0) + c'_1 p^{n-k}$  and since  $p^m G(0) < p^{n-k}$  we have  $c_1 = p^m G(0)d$ ,  $d \in \mathbb{Z}_p^\times$ . The above identity then shows that  $\wp^{p^{2m} G(0)d}$  is a principal ideal, and thus  $p^{2m} G(0)$  annihilates the class  $b_n = [\wp_n]$ . This holds for all primes above  $p$ , and since their classes generate  $\mathbf{B}_n^+$ , it holds for the whole group. Consequently  $(\mathbf{B}_n^+)^{p^{2m} G(0)} = \{1\}$  for all  $n$  and in the projective limit,  $p^{2m} G(0)$  annihilates  $\mathbf{B}^+$ . Thus  $\mathbf{B}^+$  has finite exponent and is herewith a finite module. This completes the proof of Theorems 1 and 2.  $\square$

#### 4. APPENDIX: AUXILIARY RESULTS

**4.1. Proof of Proposition 1.** The proposition is a consequence of the following elementary, technical lemma.

**Lemma 10.** *Let  $A$  and  $B$  be finitely generated abelian  $p$ -groups denoted additively, and let  $N : B \rightarrow A$ ,  $\iota : A \rightarrow B$  be two  $\mathbb{Z}_p$ -linear maps such that:*

1.  $N$  is surjective and  $\text{sexp}(A) > p$ .
2. The  $p$ -ranks of  $A$  and  $B$  are both equal to  $r$  and  $|B|/|A| = p^r$ .
3.  $N(\iota(a)) = pa, \forall a \in A$ .

*Then  $\iota$  is rank preserving, i.e.  $p\text{-rk}(\iota(A)) = p\text{-rk}(A)$ ; moreover,  $\iota(A) = pB$  and  $\text{ord}(x) = p \cdot \text{ord}(Nx)$  for all  $x \in B$ .*

*Proof.* Since  $\text{sexp}(A) > p$ , we have  $N\iota(x) = px \neq 0$  for all  $x \in A \setminus pA$ , it follows that  $p\text{-rk}(A/pA) = p\text{-rk}(\iota(A)/(p\iota(A)))$ , so  $\iota$  is rank preserving.

We start by noting that for any finite abelian  $p$ -group  $A$  of  $p$ -rank  $r$  and any pair  $\alpha_i, \beta_i$ ;  $i = 1, 2, \dots, r$  of minimal systems of generators there is a matrix  $E \in \text{Mat}(r, \mathbb{Z}_p)$  which is invertible over  $\mathbb{Z}_p$ , such that

$$(29) \quad \vec{\beta} = E\vec{\alpha}.$$

This can be verified directly by extending the map  $\alpha_i \mapsto \beta_i$  linearly to  $A$  and, since  $(\beta_i)_{i=1}^r$  is also a minimal system of generators, deducing that the map is invertible, thus regular. It represents a unimodular change of base.

The maps  $\iota$  and  $N$  induce maps

$$\bar{\iota} : A/pA \rightarrow B/pB, \quad \bar{N} : B/pB \rightarrow A/pA.$$

From 1, we see  $\bar{N}$  is surjective and since, by 2., it is a map between finite sets of the same cardinality, it is actually an isomorphism. But 3. implies that  $\bar{N} \circ \bar{\iota} : A/pA \rightarrow A/pA$  is the trivial map and since  $\bar{N}$  is an isomorphism,  $\bar{\iota}$  must be the trivial map, hence  $\iota(A) \subset pB$ .

Recall that  $\iota$  is rank preserving and let  $b_i$ ,  $i = 1, 2, \dots, r$  be a minimal set of generators of  $B$ : thus the images  $\bar{b}_i$  of  $b_i$  in  $B/pB$  form an  $\mathbb{F}_p$ -base of this algebra. Let  $a_i = N(b_i)$ ; since  $p\text{-rk}(B/pB) = p\text{-rk}(A/pA)$ , the set  $(a_i)_i$  also forms a minimal set of generators for  $A$ . We claim that  $|B/\iota(A)| = p^r$ .

Pending the proof of this equality, we show that  $\iota(A) = pB$ . Indeed, we have the equality of  $p$ -ranks:

$$|B/pB| = |A/pA| = |B/\iota(A)| = p^r,$$

implying that  $|pB| = |\iota(A)|$ ; since  $\iota(A) \subset pB$  and the  $p$ -ranks are equal, the two groups are equal, which is the first claim. The second claim will be proved after showing that  $|B/\iota(A)| = p^r$ .

Let  $S(X) = X[p] = \{x \in X : pX = 0\}$  denote the socle of the finite abelian  $p$ -group  $X$ . There is the obvious inclusion  $S(\iota(A)) \subset S(B) \subset B$  and since  $\iota$  is rank preserving,  $p\text{-rk}(A) = p\text{-rk}(S(A)) = p\text{-rk}(B) = p\text{-rk}(S(B)) = p\text{-rk}(S(\iota(A)))$ , thus  $S(B) = S(\iota(A))$ . Let  $(a_i)_{i=1}^r$  be a minimal set of generators for  $A$  and  $a'_i = \iota(a_i) \in B$ ,  $i = 1, 2, \dots, r$ ; the  $(a'_i)_{i=1}^r$  form a minimal set of generators for  $\iota(A) \subset B$ . We choose in  $B$  two systems of generators in relation to  $a'_i$  and the matrix  $E$  will map these systems according to (29).

First, let  $b_i \in B$  be such that  $p^{e_i}b_i = a'_i$  and  $e_i > 0$  is maximal among all possible choices of  $b_i$ . From the equality of socles and  $p$ -ranks, one verifies that the set  $(b_i)_{i=1}^r$  spans  $B$  as a  $\mathbb{Z}_p$ -module; moreover,  $\iota(A) \subset pB$  implies  $e_i \geq 1$ . On the other hand, the norm being surjective, there is a minimal set of generators  $b'_i \in B$ ,  $i = 1, 2, \dots, r$  such that  $N(b'_i) = a_i$ . Since  $b_i, b'_i$  span the same finite  $\mathbb{Z}_p$ -module  $B$ , (29) in which  $\vec{\alpha} = \vec{b}$  and  $\vec{\beta} = \vec{b}'$  defines a matrix with  $\vec{b} = E \cdot \vec{b}'$ . On the other hand,

$$\iota(\vec{a}) = \vec{a}' = \mathbf{Diag}(p^{e_i})\vec{b} = \mathbf{Diag}(p^{e_i})E \cdot \vec{b}',$$



The linear map  $N : B \rightarrow A$  acts component-wise on vectors  $\vec{x} \in B^r$ . Therefore,

$$\begin{aligned} N\vec{b} &= N\vec{b}_i = N(E\vec{b}') = N\left(\left(\prod_j b'_j \sum_j e_{i,j}\right)_{i=1}^r\right) \\ &= \left(\prod_j (Nb'_j)^{\sum_j e_{i,j}}\right)_{i=1}^r = \left(\prod_j (a_j)^{\sum_j e_{i,j}}\right)_{i=1}^r \\ &= E(\vec{a}). \end{aligned}$$

Using the fact that the subexponent is not  $p$ , we obtain thus two expressions for  $N\vec{a}'$  as follows:

$$\begin{aligned} N\vec{a}' &= p\vec{a} = pI \cdot \vec{a} \\ &= N\left(\mathbf{Diag}(p^{e_i})\vec{b}\right) = \mathbf{Diag}(p^{e_i}) \cdot N(\vec{b}) = \mathbf{Diag}(p^{e_i}) \cdot E\vec{a}, \quad \text{so} \\ \vec{a} &= \mathbf{Diag}(p^{e_i-1}) \cdot E\vec{a} \end{aligned}$$

The  $a_j$  form a minimal system of generators and  $E$  is regular over  $\mathbb{Z}_p$ ; therefore  $(\vec{\alpha}) := (\alpha_j)_{j=1}^r = E\vec{a}$  is also minimal system of generators of  $A$  and the last identity above becomes

$$\vec{a} = \mathbf{Diag}(p^{e_i-1}) \cdot \vec{\alpha}.$$

If  $e_i > 1$  for some  $i \leq r$ , then the right hand side is not a generating system of  $A$  while the left side is: it follows that  $e_i = 1$  for all  $i$ . Therefore  $|B/\iota(A)| = p^R$  and we have shown above that this implies the injectivity of  $\iota$ .

Finally, let  $x \in B$  and  $q = \text{ord}(Nx) \geq p$ . Then  $qN(x) = 1 = N(qx)$ , and since  $qx \in \iota(A)$ , it follows that  $N(qx) = pqx = 1$  and thus  $pq$  annihilates  $x$ . Conversely, if  $\text{ord}(x) = pq$ , then  $pqx = 1 = N(qx) = qN(x)$ , and  $\text{ord}(Nx) = q$ . Thus  $\text{ord}(x) = p \cdot \text{ord}(Nx)$  for all  $x \in B$  with  $\text{ord}(x) > p$ . If  $\text{ord}(x) = p$ , then  $x \in S(B) = S(\iota(A)) \subset \iota(A)$  and  $Nx = px = 1$ , so the last claim holds in general.  $\square$

We now give the proof of the Proposition 1:

*Proof.* Although the statement of the proposition is made in the context of the extensions of interest in this paper, the reader will note that the proof provided here holds for arbitrary base fields  $\mathbb{K}$  and arbitrary  $\Lambda$ -extensions  $\mathbb{K}_\infty/\mathbb{K}$ : this is due to the generality of Lemma 10 and of the Theorem 6 of Iwasawa [9], which will be used for the proof of the injectivity of  $\iota$ .

We first prove the existence of  $n_0$ : the module  $A^{p^m}$  is a  $\mathbb{Z}_p$ -free module, and its finite levels  $A_n^{p^m}$  have increasing  $p$ -ranks. Therefore, there is a minimal  $n_0$  such that  $p\text{-rk}(A_{n_0}^{p^m}) = p\text{-rk}(A^{p^m})$  and the rank is preserved for all  $n \geq n_0$ .

Let  $A = \Lambda a_n$  and  $B = \Lambda a_{n+1}$  in Lemma 10, and switch back to multiplicative notation. The norm will be  $N = N_{n+1,n}$  and  $\iota = \iota_{n,n+1}$ , the ideal lift map. By definition, the norm is surjective, and since  $\text{ord}(a_n) \rightarrow \infty$ , we may assume that  $\text{sexp}(A_n) > p$ . Therefore, the lemma implies that  $B^p = \iota(A)$  and for all  $x \in \Lambda a_{n+1}$  we have  $\text{ord}(x) = p \text{ord}(Nx)$ , which is the first statement in (3); the relation (4) follows from this too. Consider now  $b = a_{n+1}^{\omega_n}$ ; since  $a_{n+1}^p = \iota(a_n)$ , it follows that  $b^p = 1$ . This implies the second claim in (3).

The ideal lift map is injective on  $A_n^-$  and since  $A = A^- \cdot A^+$ , it suffices to consider the injectivity of  $\iota_{n,n+1}$  for  $a = (a_n)_{n \in \mathbb{N}} \in A^+$ . For the case  $a \in A^+$  we shall give a proof using an argument of Fukuda from [7]. Suppose that  $\Lambda a$  is a free  $\mathbb{Z}_p$ -module, so the rank is necessarily finite. Suppose that the claim is false; then for all  $n > 0$  there is an  $m > n$  such that  $\iota_{m,m+1}$  is not injective. Since the rank of  $\Lambda a$  is finite, for all  $m > 0$ , there is a  $b \in \Lambda a$  and an  $n > m$  such that  $\text{ord}(\iota(b_n^{T^i})) < \text{ord}(b_n^{T^i})$  for  $i = 0, 1, \dots, p\text{-rk}(\Lambda b_n) - 1$ . In particular  $\Lambda b_n \cong \Lambda b_{n+1}$ , since  $N \circ \iota = p$  and  $\iota(\Lambda b_n) = \Lambda b_{n+1}^p$  by Lemma 10. We show that  $\Lambda b$  is finite, which contradicts the fact that  $\Lambda a$  is a free  $\mathbb{Z}_p$ -module. For this we shall use a variant of Iwasawa's Theorem 6 in [9] (see also [21], Lemma 13.15). There is an  $M > 0$  such that  $A^{p^M} = \bigoplus_{i=1}^t \Lambda(a^{(i)})^{p^M}$  is a direct sum of free  $\mathbb{Z}_p$ -modules: it suffices to take  $M$  large enough, so that it annihilates both the  $\mathbb{Z}_p$  torsion of  $A$  and the kernels and cokernels in the pseudoisomorphism  $A \sim \bigoplus \Lambda/(f_j)$ . Let  $m > 2M$ , say, and for  $n \geq m$  let  $\mathbb{F}_n \subset \mathbb{H}_n$  be the fixed field of  $\varphi(A^{p^M})$ . We may assume without restriction of generality that  $a = a^{(1)}$  and let  $A(a) = \bigoplus_{i=2}^t \Lambda(a^{(i)})^{p^M}$  be the complement of  $a^{(1)}$ . We then define  $\mathbb{F}_{n,a} = \mathbb{H}_n^{\varphi(A(a))}$ . Then  $\mathbb{F}_{n,a}/\mathbb{F}_n$  is an unramified extension with group  $\text{Gal}(\mathbb{F}_{n,a}/\mathbb{F}_n) \cong (\Lambda a)^{p^M}$ . Following the proof of Theorem 6, we let  $\overline{G} = \text{Gal}(\mathbb{H}/\mathbb{K})$  and  $I_\nu \subset \overline{G}$  be the inertia groups of some primes  $\mathfrak{P}_\nu \subset \mathbb{H}$  above  $\nu\wp$ , for  $\nu \in C$ . Let  $\tilde{\Gamma} = I_1$  be a lift of  $\Gamma$  to  $\overline{G}$  and  $\tilde{\tau} \in \tilde{\Gamma}$  a topological generator that restricts to  $\tau \in \Gamma$ .

Let  $\mathbb{F} = \bigcup_n \mathbb{F}_n$  and  $\mathbb{F}_a = \bigcup_n \mathbb{F}_{n,a}$ , both subfields of  $\mathbb{H}$  with  $\text{Gal}(\mathbb{F}_a/\mathbb{F}) \cong (\Lambda a)^{p^M}$ . Let  $G = \text{Gal}(\mathbb{F}_a/\mathbb{F}_m)$ ,  $X = \text{Gal}(\mathbb{F}_a/\mathbb{F})$  and identify  $\tilde{\Gamma}$  with its restriction to  $G$ . Let  $g \in \mathbb{Z}_p[T]$  be such that  $b = a^g$ , so  $\Lambda b_n^{p^M} = \Lambda a_n^{gp^M}$ . Let

$$Y_n = \varphi \left( \text{Ker} (N : \Lambda b_n^{p^M} \rightarrow \Lambda b_n^{p^M}) \right) \subset X^g,$$

so  $\Lambda b_n^{p^M} \cong X^g/Y_n$ . It follows from Iwasawa's proof that  $\varphi(Y)_n = \nu_{n,m}(\varphi(Y)_m)$  for all  $n \geq m$ , and since the Artin map is bijective, we also have  $Y_n = \nu_{n,m}Y_m$ . Let  $\mathcal{M} = \Lambda b^{p^M}$  and  $\mathcal{M}_n = \Lambda b_n^{p^M}$ . From the choice of  $Y_n$ , we have a commutative diagram in which  $\mathcal{M}_n \rightarrow \mathcal{M}_m$  is induced by the map  $N_{n,m}$  while the horizontal isomorphism are deduced from the definition of  $Y_n$ .

$$(30) \quad \begin{array}{ccc} \mathcal{M}_n & \cong & \mathcal{M}/\nu_{n,m}Y_m \\ \downarrow & & \downarrow \\ \mathcal{M}_m & \cong & \mathcal{M}/Y_m. \end{array}$$

We assumed that  $|\mathcal{M}_{m+1}| = |\mathcal{M}_m|$ . Then  $\mathcal{M}_{m+1} \rightarrow \mathcal{M}_m$  is an isomorphism of finite abelian  $p$ -groups; therefore  $\nu_{m+1,m} Y_m = Y_m$ . Since  $\mathfrak{M} = (p, T) \subset \Lambda$  is the unique maximal ideal and  $\nu_{m+1,m} \in \mathfrak{M}$ , and since  $Y_m$  is finitely generated over  $\Lambda$ , it follows from Nakayama's lemma that  $Y_m = \{1\}$ . Consequently,  $\mathcal{M} \cong \mathcal{M}_m$  is finite. But  $\mathcal{M} \subset \Lambda a^{p^M}$ , which is a  $\mathbb{Z}_p$ -free  $\Lambda$ -module, so we must have  $b = 1$ . It follows that for sufficiently large  $n$ , the ideal lift map is injective on all  $\mathbb{Z}_p$ -free  $\Lambda$ -submodules of  $A$ , which completes the proof.  $\square$

#### 4.2. Proof of Proposition 2.

*Proof of Proposition 2.* Let  $\Omega_n$  denote here the maximal  $p$ -ramified  $p$ -abelian extension of  $\mathbb{K}_n$  and  $\Omega'_n \subset \Omega_n^-$  be the maximal Kummer extension contained in  $\Omega_n^-$ .

The radical  $\text{Rad}(\Omega'_n/\mathbb{K}_\infty)$  is annihilated by  $\omega_n^*$ . The action of the Iwasawa involution on  $\omega_n$  is seen from  $(T+1)^{p^{n-k}} \omega_n^* + \omega_n = (p^k - 1)^{p^{n-k}} - 1$ ; it follows that:

$$(31) \quad \omega_n + t\omega_n^* = p^{n-k}c, \quad t \in \Lambda_n^\times, c \in \mathbb{Z}_p^\times.$$

We define for  $m > n$ :  $\mathcal{E}'_m = \{e^{N_{m,n}^*} : e \in E_m\}$  and  $\mathcal{E}_m = \mathcal{E}'_m \cdot (E_m)^{p^m}$ . Then

$$(32) \quad \Omega_n^- \supset \mathbb{H}_n \cdot \cup_m \mathbb{K}_m[\mathcal{E}_m^{1/p^m}].$$

By comparing galois groups we shall show that  $\Omega_n^- = \mathbb{K}_n \cdot \mathbb{K}_m[\mathcal{E}_m^{1/p^m}] \cdot \mathbb{T}_n$ , where  $\mathbb{T}_n/\mathbb{K}_n$  is an extension with group  $\text{Gal}(\mathbb{T}_n/\mathbb{K}_n) \cong (\mathbb{Z}/(p^n \cdot \mathbb{Z}))^{s-1}$ ,  $s = |C|$ , which shall be described in the proof.

Since  $\mathbb{U}_n^- \cap \overline{E}_n = \mu_{p^n}$ , it follows that  $\text{Gal}(\Omega_n/\mathbb{H}_n) = U_n^- \times \mathcal{T}(U_n^-)/\mu_{p^n}$ , where the torsion part  $\mathcal{T}(U_n^-) = \prod_{\nu \in C} \mu_{p^n}$  is the product of the images of the  $p^n$ -th roots of unity in the single completions, factored by the diagonal embedding of the global units. We shall show that  $\text{Gal}(\Omega_n^-/\Omega_E \cdot \mathbb{H}_n) \cong \mathcal{T}(U_n^-)/\mu_{p^n}$ .

For the proof, we need to verify that ranks are equal on both sides. Let  $\pi_\nu \in \mathbb{K}_n$  be a list of integers such that  $(\pi_\nu) = \wp^{\nu h}$  for  $h$  the order of the class of  $\wp^\nu$ , for  $\wp \supset (p)$  some fixed prime of  $\mathbb{K}_n$ . Then we see that  $\mathbb{T}_n = \prod_{\nu \in C} \mathbb{K}_n[\pi_\nu^{1/p^{n+1}}]$  is a  $p$ -ramified extension with group  $\text{Gal}(\mathbb{T}_n/\mathbb{K}_n) = \mathcal{T}(U_n^-)/\mu_{p^n} \subset \text{Gal}(\Omega_n/\mathbb{H}_n)$ .

A straight forward computation in the group ring yields that

$$(33) \quad \omega_n^* x \equiv 0 \pmod{(\omega_m, p^m)\Lambda}, \quad \text{if } x \in N_{m,n}^* \Lambda.$$

On the other hand, suppose that  $e \in \text{rad}((\Omega_n \mathbb{K}_m)/\mathbb{K}_m) \cap E_m$ : the previous observation and Kummer theory imply that  $e^{\omega_n^*} \in \mathcal{E}'_m$ . Therefore  $\mathbb{F} := \cup_m \mathbb{K}_m[\mathcal{E}_m^{1/p^m}] = \Omega_n^- \cap \Omega_E$ . We now show that  $\mathbb{Z}_p\text{-rk}(\mathbb{F}/\mathbb{K}_\infty) = r_2(\mathbb{K}_n)$ . Let  $H_0, H_1, \dots, H_{r_2-1} \in E_m$  build a base for the  $\mathbb{F}_p$ -vector space  $E_m/E_m^{(p,T)}$ : after an eventual change of  $\mathbb{Z}$ -base, we may assume that  $N_{m,n}(H_0) = 1$  while  $N_{m,n}(H_i) \in e_i^{\mathbb{Z}}, i = 1, 2, \dots, r_2 - 1$  have minimal  $p$ -index, for a Dirichlet base  $e_1, e_2, \dots, e_{r_2-1} \in E_n$ . The units  $H_0$  are then a system of Hilbert

relative units, in the sense of Hilbert's Theorem 91. Let  $\mathcal{F}'_m = [H_i^{N_{m,n}^*} : i = 0, 1, \dots, r_2 - 1]_{\mathbb{Z}[T^*]} \subset \mathcal{E}'_m$ . Assume that  $m = 2m'$ ; we show that  $\mathcal{F}_m/(E_m^{p^{m'}} \cap \mathcal{F}_m)$  has  $p$ -rank  $r_2$ . First  $(\mathcal{F}')_m^{\omega_m^*} \subset E_m^{p^m}$  by (33), so  $p\text{-rk}(\mathcal{F}_m) \leq r_2$ . We now use the following observation of B. Anglès [2], Lemma 2.1, (2): let  $m = k + l$  and  $l' = \lfloor l/2 \rfloor$ . Then

$$\omega_m(T) = TN_{m,k} \in (p^{l'}, T^{p^{l'+1}}).$$

We may thus choose  $a, b \in \Lambda_m$  with  $a \in \Lambda_m^\times$  such that

$$(34) \quad N_{m,k}^* = ap^{l'} + bN_{l'+1,k}.$$

It follows that for  $x \in \mathbb{K}_m^\times \setminus (\mathbb{K}_m^\times)^p$  we have  $x^{N_{m,k}^*} \notin (\mathbb{K}_m^\times)^{p^{m'+1}}$  and a fortiori,

$$x^{N_{m,n}^*} \notin (\mathbb{K}_m^\times)^{p^{m'+1}},$$

which implies for sufficiently large  $m = 2m'$ , that  $\mathcal{F}'_m/(E_m^{p^{m'}+n} \cap \mathcal{F}'_m)$  has  $p$ -rank  $r_2$ . We have  $\mathbb{F}_m := \mathbb{K}_m[E_m^{N_{m,n}^*/p^m}] \supseteq \mathbb{F}'_m := \mathbb{K}_m[\mathcal{F}_m^{1/p^m}]$  and  $\mathbb{F} = \cup_m \mathbb{F}_m$ . The previous computations show that

$$\begin{aligned} \text{sexp}(\text{Gal}(\mathbb{F}_m/\mathbb{K}_m)) &\geq \text{sexp}(\text{Gal}(\mathbb{F}'_m/\mathbb{K}_m)) \geq p^{m'-n} \quad \text{and} \\ r_2 &\geq p\text{-rk}(\text{Gal}(\mathbb{F}_m/\mathbb{K}_m)) \geq p\text{-rk}(\text{Gal}(\mathbb{F}'_m/\mathbb{K}_m)) = r_2. \end{aligned}$$

In particular, the subexponents of  $\text{Gal}(\mathbb{F}'_m/\mathbb{K}_m)$  are divergent. Moreover  $\mathbb{F}_m \subset \mathbb{F}_{m+1}$  for all  $m$ . Consequently,  $\mathbb{F}/\mathbb{K}_\infty$  is a product of  $r_2$  independent  $\mathbb{Z}_p$ -extensions.

Comparing ranks, we see that

$$\text{ess. } p\text{-rk}(\text{Gal}(\Omega_n^-/(\mathbb{K}_\infty \cdot \mathbb{H}_n))) = r_2 = \text{ess. } p\text{-rk}(\text{Gal}(\mathbb{F}/\mathbb{K}_\infty)).$$

It follows that  $\Omega_n^- \supseteq \mathbb{F} \cdot \mathbb{T}_n \cdot \mathbb{H}_n$  and  $\text{Gal}((\mathbb{F} \cdot \mathbb{T}_n \cdot \mathbb{H}_n)/\mathbb{H}_n) \sim \text{Gal}(\Omega_n^-/\mathbb{H}_n)$ . In particular,  $\Omega_n^- \cap \Omega_{E'} = \mathbb{T}_n \cdot \mathbb{F}$ . Therefore if the previous inclusion is strict, then  $1 < [\Omega_n^- \cdot \Omega_{E'} : \Omega_{E'}] < \infty$ . But  $\text{Gal}(\Omega_n^-/\Omega_{E'})$  is a  $\mathbb{Z}_p$ -free  $\Lambda$ -torsion module and thus  $\Omega_n^-$  contains no finite, totally ramified subextensions of  $\Omega_{E'}$ . It follows that  $\Omega_n^- = \mathbb{H}_n \cdot \mathbb{F} \cdot \mathbb{T}_n \subset \Omega_{E'} \cdot \mathbb{H}_n$ , which completes the proof of the proposition.  $\square$

**Acknowledgments:** I thank all my colleagues in Göttingen for their support and motivating discussions; my gratitude goes in particular to Laurent Bartholdi, Tobias Bembom, Oliver Bräunling, Christian Böhning, Machiel van Fankenhuijsen, Ina Kersten, Ralf Meyer, Gabriele Ranieri, Thomas Schick and Victor Vuletescu. I am most grateful to Samuel Patterson who followed during a seminar in summer 2008 the development of some of the ideas presented here, with his attention, remarks and advice.

During the elaboration of this final version of my paper, a list of international colleagues have given their support with useful discussions, encouraging comments and/or careful reading of intermediate versions. I wish to express my gratitude here to Bruno Anglès, John Coates, Ralf Greenberg,

Minhyong Kim, Hendrik Lenstra, Francesco Pappalardi, Vicențiu Pașol, Florian Pop, Ehud De Shalit and George Walker.

Last but not least I thank Theres and Seraina for the innocent patience with which they dealt with my ambig presence over longer periods of time: sometimes ramified, sometimes simply capitulated.

## REFERENCES

- [1] T. Albu. *Cogalois theory*. Number 252 in Monographs and textbooks in pure and applied mathematics. Marcel Dekker Inc., 2003.
- [2] B. Anglès. On the  $p$ -adic Leopoldt transformation of a power series. *Acta Arithmetica*, 134(4):349–368, 2008.
- [3] J. Ax. On the units of an algebraic number field. *Illinois Journal of Mathematics*, 9:584–589, 1965.
- [4] A. Baker. Linear forms in the logarithms of algebraic numbers I, II, III. *Mathematika*, 13, 14:204–216; 102–107, 220–228, 1966, 67.
- [5] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.
- [6] M. Emsalem, H. Kisilevsky, and D. Wales. Indépendance linéaire sur  $\overline{\mathbb{Q}}$  de logarithmes  $p$ -adiques de nombres algébriques et rang  $p$ -adique du groupe des unités d'un corps de nombres. *Journal of Number Theory*, 19:384–391, 1984.
- [7] T. Fukuda. Remarks on  $\mathbb{Z}_p$ -extensions of number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(8):264–266, 1994.
- [8] R. Greenberg. On the Iwasawa invariants of totally real fields. *American Journal of Mathematics*, 98:263–284, 1976.
- [9] K. Iwasawa. On  $\mathbb{Z}_\ell$ -extensions of number fields. *Ann. Math. Second Series*, 98:247–326, 1973.
- [10] G. Janusz. *Algebraic Number Fields*. Academic Press, 1973.
- [11] J. Jaulent. Note sur la conjecture de Leopoldt. <http://front.math.ucdavis.edu/0712.2995>, 2007.
- [12] M. Laurent. Rang  $p$ -adique d'unités et action de groupes. *J. reine angew. Math.*, 399:81–108, 1989.
- [13] H. Leopoldt. Zur Arithmetik in Abelschen Zahlkörper. *J. Reine Angew. Math*, 209:54–71, 1962.
- [14] P. Mihăilescu. SNOQIT II: Units and Kummer Theory in Iwasawa extensions. Math. Arxiv, Sept. 2010. <http://arxiv.org/abs/1009.3729v1>.
- [15] P. Mihăilescu. The  $T$  and  $T^*$  components of  $\Lambda$ -modules and Leopoldt's conjecture. Math. Arxiv, Sept. 2010. <http://front.math.ucdavis.edu/0905.1274>.
- [16] P. Mihăilescu. Iwasawa's constant  $\mu$  vanishes in cyclotomic  $\mathbb{Z}_p$ -extensions of CM fields. Math. Arxiv, May 2011. <http://front.math.ucdavis.edu/1105.1970>.
- [17] P. Mihăilescu. Snoqit I: Growth of  $\Lambda$ -modules and Kummer theory. Math. Arxiv, May 2011. <http://front.math.ucdavis.edu/1105.5989>.
- [18] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer, 1986.
- [19] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer, combined Second Edition edition, 1990.
- [20] M. Waldschmidt. Transcendence et exponentielles en plusieurs variables. *Inventiones Mathematicae*, 63, 1981.
- [21] L. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1996.

(P. Mihăilescu) MATHEMATISCHES INSTITUT DER UNIVERSITÄT GÖTTINGEN  
*E-mail address*, P. Mihăilescu: [preda@uni-math.gwdg.de](mailto:preda@uni-math.gwdg.de)